

Лабораторная работа №6

Дисциплина: Информационная безопасность

Дорофеева Алёна Тимофеевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
4.1	Подготовительный этап	9
4.2	Порядок выполнения работы	11
5	Выводы	26
	Список литературы	27

Список иллюстраций

4.1	Проверка политики и режима	9
4.2	Обновление	10
4.3	Загрузка Apache	10
4.4	Расположение конфигурационного файла httpd	10
4.5	Задаем ServerName	11
4.6	Задаем ServerName	11
4.7	Режим enforcing политики targeted	12
4.8	Запуск	12
4.9	Контекст безопасности	13
4.10	Переключатели SELinux для Apache	14
4.11	Статистика по политике	15
4.12	Типы файлов	15
4.13	Типы файлов	16
4.14	Создание html файла	16
4.15	Создание html файла	17
4.16	Обращение к файлу через веб-сервер	17
4.17	Контекст безопасности html файла	18
4.18	Смена контекста безопасности html файла	18
4.19	Попытка получения доступа к файлу через веб-сервер	18
4.20	tail /var/log/messages	19
4.21	/var/log/audit/audit.log	20
4.22	Смена прослушиваемого порта	20
4.23	Перезапуск Apache	21
4.24	tail -nl /var/log/messages	21
4.25	/var/log/http/error_log	21
4.26	/var/log/http/access_log	22
4.27	/var/log/audit/audit.log	22
4.28	Список портов	22
4.29	Запуск веб-сервера	23
4.30	Возвращаем контекст безопасности	23
4.31	Получение доступа к файлу через веб-сервер	24
4.32	Изменение прослушиваемого порта	24
4.33	Удаление файла	25

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 Задание

- Изучить на практике работу SELinux и Apache.

3 Теоретическое введение

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена.

Для того, чтобы понять, в чем состоит практическая ценность SELinux, рассмотрим несколько примеров, когда стандартная система контроля доступа недостаточна. Если SELinux отключен, то вам доступна только классическая дискреционная система контроля доступа, которая включает в себя DAC (избирательное управление доступом) или ACL(списки контроля доступа). То есть речь идет о манипулировании правами на запись, чтение и исполнение на уровне пользователей и групп пользователей, чего в некоторых случаях может быть совершенно недостаточно. Например:

- Администратор не может в полной мере контролировать действия пользователя. Например, пользователь вполне способен дать всем остальным пользователям права на чтение собственных конфиденциальных файлов, таких как ключи SSH.
- Процессы могут изменять настройки безопасности. Например, файлы, содержащие в себе почту пользователя должны быть доступны для чтения

только одному конкретному пользователю, но почтовый клиент вполне может изменить права доступа так, что эти файлы будут доступны для чтения всем.

- Процессы наследуют права пользователя, который их запустил. Например, зараженная трояном версия браузера Firefox в состоянии читать SSH-ключи пользователя, хотя не имеет для того никаких оснований.[01?]

Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.[02?]

Установить веб-сервер Apache можно следующим образом. Откройте окно терминала и обновите списки пакетов репозитория, введя следующее: `sudo yum update`

Теперь вы можете установить Apache с помощью команды: `sudo yum -y install httpd`

httpd - это имя службы Apache в CentOS. Опция `-y` автоматически отвечает да на запрос подтверждения.[03?]

4 Выполнение лабораторной работы

4.1 Подготовительный этап

Сперва проверим конфигурационный файл SELinux - видим, что политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется (рис. 4.1).

```
[aldoro@aldoro ~]$ su -
Password:
[root@aldoro ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started-with-selinux-selinux-states-and-modes
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted

[root@aldoro ~]#
```

Рис. 4.1: Проверка политики и режима

Дальше потребуется установить менеджер Apache, для этого предварительно обновим систему (рис. 4.2), только после этого устанавливаем Apache (httpd) (рис. 4.3).

```
[root@aldoro ~]# yum update
Last metadata expiration check: 1:18:57 ago on Thu 12 Oct 2023 05:05:31 AM MSK.
Dependencies resolved.
=====
Package Arch Version Repository Size
=====
Installing:
kernel x86_64 5.14.0-284.30.1.el9_2 baseos 3.4 M
Upgrading:
NetworkManager x86_64 1:1.42.2-8.el9_2 baseos 2.2 M
NetworkManager-adsl x86_64 1:1.42.2-8.el9_2 baseos 32 k
NetworkManager-bluetooth x86_64 1:1.42.2-8.el9_2 baseos 58 k
NetworkManager-config-server noarch 1:1.42.2-8.el9_2 baseos 18 k
NetworkManager-libnm x86_64 1:1.42.2-8.el9_2 baseos 1.8 M
NetworkManager-team x86_64 1:1.42.2-8.el9_2 baseos 37 k
NetworkManager-tui x86_64 1:1.42.2-8.el9_2 baseos 239 k
NetworkManager-wifi x86_64 1:1.42.2-8.el9_2 baseos 78 k
NetworkManager-wwan x86_64 1:1.42.2-8.el9_2 baseos 65 k
avahi x86_64 0.8-12.el9_2.1 baseos 287 k
avahi-glib x86_64 0.8-12.el9_2.1 appstream 13 k
avahi-libs x86_64 0.8-12.el9_2.1 baseos 66 k
bind-libs x86_64 32:9.16.23-11.el9_2.1 appstream 1.2 M
```

Рис. 4.2: Обновление

```
[root@aldoro ~]# yum install httpd
Last metadata expiration check: 1:42:45 ago on Thu 12 Oct 2023 05:05:31 AM MSK.
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
httpd x86_64 2.4.53-11.el9_2.5 appstream 47 k
Installing dependencies:
apr x86_64 1.7.0-11.el9 appstream 123 k
apr-util x86_64 1.6.1-20.el9_2.1 appstream 94 k
apr-util-bdb x86_64 1.6.1-20.el9_2.1 appstream 12 k
httpd-core x86_64 2.4.53-11.el9_2.5 appstream 1.4 M
httpd-filesystem noarch 2.4.53-11.el9_2.5 appstream 14 k
httpd-tools x86_64 2.4.53-11.el9_2.5 appstream 81 k
rocky-logos-httpd noarch 90.14-1.el9 appstream 24 k
Installing weak dependencies:
apr-util-openssl x86_64 1.6.1-20.el9_2.1 appstream 14 k
mod_http2 x86_64 1.15.19-4.el9_2.4 appstream 149 k
mod_lua x86_64 2.4.53-11.el9_2.5 appstream 61 k

Transaction Summary
-----
Install 11 Packages

Total download size: 2.0 M
Installed size: 5.9 M
Is this ok [y/N]: y
Downloading Packages:
```

Рис. 4.3: Загрузка Apache

Далее зададим ServerName test.ru в конфигурационном файле httpd (рис. 4.5), для этого сперва найдем, где он находится (рис. 4.4).

```
[root@aldoro ~]# ls /etc/httpd
conf conf.d conf.modules.d logs modules run state
[root@aldoro ~]# ls /etc/httpd/conf
httpd.conf magic
[root@aldoro ~]# nano /etc/httpd/conf/httpd.conf
```

Рис. 4.4: Расположение конфигурационного файла httpd

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
ServerName test.ru
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>
#
# Note that from this point forward you must specifically allow
```

Рис. 4.5: Задаем ServerName

Чтобы пакетный фильтр в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp добавим разрешающие правила (рис. 4.6):

```
[root@aldoro ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@aldoro ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@aldoro ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@aldoro ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@aldoro ~]#
```

Рис. 4.6: Задаем ServerName

4.2 Порядок выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис. 4.7).

```

[aldoro@aldoro ~]$ getenforce
Enforcing
[aldoro@aldoro ~]$ 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
[aldoro@aldoro ~]$

```

Рис. 4.7: Режим enforcing политики targeted

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status`. Видим, что он неактивен, поэтому запускаем его командой `service httpd start`, после чего снова проверяем, в этот раз сервис активен (рис. 4.9).

```

[aldoro@aldoro ~]$ 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)
[aldoro@aldoro ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[aldoro@aldoro ~]$ 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 Thu 2023-10-12 07:02:26 MSK; 16s ago
     Docs: man:httpd.service(8)
  Main PID: 109637 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 12221)
   Memory: 23.2M
      CPU: 108ms
    CGroup: /system.slice/httpd.service
            └─109637 /usr/sbin/httpd -DFOREGROUND
              └─109642 /usr/sbin/httpd -DFOREGROUND
                └─109648 /usr/sbin/httpd -DFOREGROUND
                  └─109649 /usr/sbin/httpd -DFOREGROUND
                    └─109650 /usr/sbin/httpd -DFOREGROUND

Oct 12 07:02:26 aldoro.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 12 07:02:26 aldoro.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 12 07:02:26 aldoro.localdomain httpd[109637]: Server configured, listening on: port 80
[aldoro@aldoro ~]$

```

Рис. 4.8: Запуск

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно ис-

пользовать команду `ps auxZ | grep httpd` (4.9).

```
[aldoro@aldoro ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 109637 0.0 0.5 20116 11492 ? Ss 07:02 0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 109642 0.0 0.3 21600 7256 ? S 07:02 0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 109648 0.0 0.5 1538124 11012 ? Sl 07:02 0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 109649 0.0 0.5 1538124 11012 ? Sl 07:02 0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 109650 0.0 0.6 1669260 13060 ? Sl 07:02 0:00 /usr/sb
in/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 aldoro 109904 0.0 0.1 221664 2320 pts/0 S+ 07:03
0:00 grep --color=auto httpd
[aldoro@aldoro ~]$
```

Рис. 4.9: Контекст безопасности

Видим, что веб-сервер имеет контекст безопасности `httpd_t`.

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b httpd` (рис. 4.10). Многие из них находятся в положении «off».

```

[aldoro@aldoro ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system     off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write              off
cobbler_can_network_connect    off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect   off
colord_use_nfs                  off
condor_tcp_network_connect     off
conman_can_network             off
conman_use_nfs                  off
container_connect_any          off
container_manage_cgroup        off
container_use_cephfs           off
container_use_devices          off
container_use_ecryptfs         off
cron_can_relabel               off
cron_system_cronjob_use_shares off

```

Рис. 4.10: Переключатели SELinux для Apache

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. 4.11).

```
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:        5100     Attributes:      258
Users:        8       Roles:          14
Booleans:     353     Cond. Expr.:    384
Allow:        65008   Neverallow:     0
Auditallow:   170     Dontaudit:      8572
Type_trans:   265344  Type_change:    87
Type_member:  35      Range_trans:    6164
Role allow:   38      Role_trans:     420
Constraints:  70      Validatetrans:  0
MLS Constrai: 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:       660
Netifcon:     0      Nodecon:       0

[aldoro@aldoro ~]$
```

Рис. 4.11: Статистика по политике

Число пользователей = 8, ролей = 14, типов = 5100.

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 4.12).

```
[aldoro@aldoro ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
[aldoro@aldoro ~]$
```

Рис. 4.12: Типы файлов

В каталоге находятся только директории.

7. Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. 4.13).

```
[aldoro@aldoro ~]$ ls -lZ /var/www/html
total 0
[aldoro@aldoro ~]$
```

Рис. 4.13: Типы файлов

Директория пуста.

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html - это только пользователь root.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 4.14):

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

```
[aldoro@aldoro ~]$ su -
Password:
[root@aldoro ~]# nano /var/www/html/test.html
[root@aldoro ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@aldoro ~]#
```

Рис. 4.14: Создание html файла

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 4.15).


```
[aldoro@aldoro ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 12 07:14 test.html
[aldoro@aldoro ~]$
```

Рис. 4.15: Создание html файла

Контекст безопасности - **httpd_sys_content_t**.

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 4.16). Файл был успешно отображён.

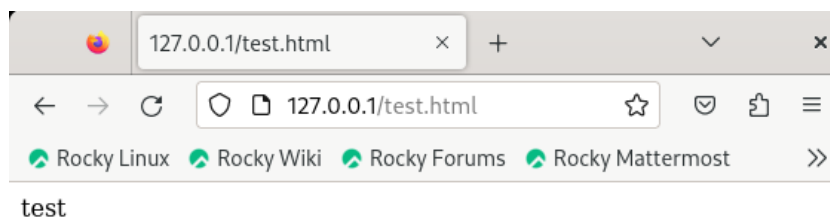


Рис. 4.16: Обращение к файлу через веб-сервер

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`.

Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z /var/www/html/test.html` (рис. 4.17). Контекст безопасности файла - **httpd_sys_content_t**. Данный контекст входит в перечень контекстов безопасности `httpd`.

Роль **object_r** используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип **httpd_sys_content_t** позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

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

Рис. 4.17: Контекст безопасности html файла

13. Измените 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 (рис. 4.18):

```
chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
```

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

Рис. 4.18: Смена контекста безопасности html файла

Видим, что контекст безопасности действительно изменился.

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 4.19).

Мы получили сообщение об ошибке: **Forbidden You don't have permission to access /test.html on this server.**

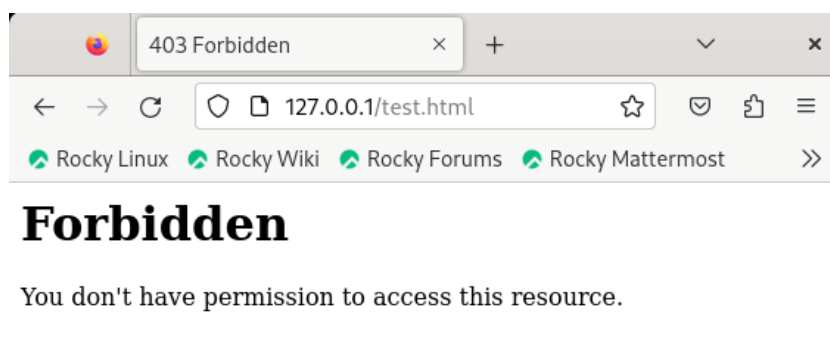


Рис. 4.19: Попытка получения доступа к файлу через веб-сервер

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?
`ls -l /var/www/html/test.html` (рис. ??) - нет доступа к файлу из-за недопустимого контекста безопасности для httpd.

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` (рис. ??).

Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd` (рис. ??), то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log` (рис. ??).

```
[root@aldoro ~]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 Oct 12 07:14 /var/www/html/test.html
[root@aldoro ~]# tail /var/log/messages
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /va
r/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If yo
u want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run re
storecon. 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 pub
lic content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# sem
ange fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***
* Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be al
lowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a lo
cal policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw
| audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /va
r/www/html/test.html. For complete SELinux messages run: sealert -l 75b759cf-8678-4b72-91d7-4828e4b3e437
Oct 12 07:26:35 aldoro setroubleshoot[111056]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /va
r/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If yo
u want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run re
storecon. 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 pub
lic content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# sem
ange fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***
* Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be al
lowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a lo
cal policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw
| audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 07:26:45 aldoro systemd[1]: dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfu
lly.
Oct 12 07:26:45 aldoro systemd[1]: dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.365s CPU ti
me.
Oct 12 07:26:45 aldoro systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 12 07:26:45 aldoro systemd[1]: setroubleshootd.service: Consumed 1.443s CPU time.
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct:backend::ffi] Missing HTTP status
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct:backend::ffi] Missing HTTP status
Oct 12 07:27:00 aldoro systemd[1574]: app-gnome-firefox-110770.scope: Consumed 22.636s CPU time.
[root@aldoro ~]#
```

Рис. 4.20: `tail /var/log/messages`

```
[root@aldoro ~]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1697071700.305:9504): op=start ver=3.0.7 format=enriched kernel=5.14.0-284.11.1.el9_2.x86_64
aid=4294967295 pid=712 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUDID="unset" UID="root"
type=SERVICE_START msg=audit(1697071700.311:5): pid=1 uid=0 aid=4294967295 ses=4294967295 subj=system_u:system_r:init_t
:s0 msg=unit=systemd-journald-catalog-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=?
res=successUID="root" AUDID="unset"
type=CONFIG_CHANGE msg=audit(1697071700.355:6): op=set audit_backlog_limit=8192 old=64 aid=4294967295 ses=4294967295 su
bj=system_u:system_r:unconfined_service_t:s0 res=1AUDID="unset"
type=SYSCALL msg=audit(1697071700.355:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04ff7720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=
sendto AUDID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1697071700.355:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469
742E72756C6573
type=CONFIG_CHANGE msg=audit(1697071700.355:7): op=set audit_failure=1 old=1 aid=4294967295 ses=4294967295 subj=system_
u:system_r:unconfined_service_t:s0 res=1AUDID="unset"
type=SYSCALL msg=audit(1697071700.355:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04ff7720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=
sendto AUDID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1697071700.355:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469
742E72756C6573
type=CONFIG_CHANGE msg=audit(1697071700.355:8): op=set audit_backlog_wait_time=60000 old=60000 aid=4294967295 ses=42949
67295 subj=system_u:system_r:unconfined_service_t:s0 res=1AUDID="unset"
type=SYSCALL msg=audit(1697071700.355:8): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04ff7720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
```

Рис. 4.21: /var/log/audit/audit.log

16. Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81 (рис. 4.22).

```
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
#Listen 80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO yo
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
```

Рис. 4.22: Смена прослушиваемого порта

17. Выполните перезапуск веб-сервера Apache (рис. 4.23). Произошёл сбой? Поясните почему?

```
[root@aldoro ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@aldoro ~]#
```

Рис. 4.23: Перезапуск Apache

Ошибки не возникает, поскольку в изначальных настройках системы порт 81 уже был прописан в рекомендациях системы.

18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` - нет никаких ошибок (рис. 4.24). Просмотрите файлы `/var/log/http/error_log` (рис. 4.25), `/var/log/http/access_log` (рис. 4.26) и `/var/log/audit/audit.log` (рис. 4.27) и выясните, в каких файлах появились записи - нет записей об ошибках, т.к. нет ошибок.

```
[root@aldoro ~]# tail /var/log/messages
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 12 07:26:59 aldoro firefox.desktop[110770]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 12 07:27:00 aldoro systemd[1574]: app-gnome-firefox-110770.scope: Consumed 22.636s CPU time.
Oct 12 07:40:10 aldoro systemd[1]: Stopping The Apache HTTP Server...
Oct 12 07:40:12 aldoro systemd[1]: httpd.service: Deactivated successfully.
Oct 12 07:40:12 aldoro systemd[1]: Stopped The Apache HTTP Server.
Oct 12 07:40:12 aldoro systemd[1]: httpd.service: Consumed 1.843s CPU time.
Oct 12 07:40:12 aldoro systemd[1]: Starting The Apache HTTP Server...
Oct 12 07:40:12 aldoro systemd[1]: Started The Apache HTTP Server.
Oct 12 07:40:12 aldoro httpd[111134]: Server configured, listening on: port 81
[root@aldoro ~]#
```

Рис. 4.24: `tail -nl /var/log/messages`

```
[root@aldoro ~]# cat /var/log/httpd/error_log
[Thu Oct 12 07:02:26.171936 2023] [core:notice] [pid 109637:tid 109637] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Thu Oct 12 07:02:26.181006 2023] [suexec:notice] [pid 109637:tid 109637] AH01232: suEXEC mechanism enabled (wrapper: /u
sr/sbin/suexec)
[Thu Oct 12 07:02:26.203377 2023] [lbmethod_heartbeat:notice] [pid 109637:tid 109637] AH02282: No slotmem from mod_heart
monitor
[Thu Oct 12 07:02:26.220683 2023] [mpm_event:notice] [pid 109637:tid 109637] AH00489: Apache/2.4.53 (Rocky Linux) config
ured -- resuming normal operations
[Thu Oct 12 07:02:26.220724 2023] [core:notice] [pid 109637:tid 109637] AH00094: Command line: '/usr/sbin/httpd -D FOREG
ROUND'
[Thu Oct 12 07:26:30.610067 2023] [core:error] [pid 109648:tid 109823] (13)Permission denied: [client 127.0.0.1:47686] A
H00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing o
n a component of the path
[Thu Oct 12 07:40:10.965630 2023] [mpm_event:notice] [pid 109637:tid 109637] AH00492: caught SIGWINCH, shutting down gra
cefully
[Thu Oct 12 07:40:12.124939 2023] [core:notice] [pid 111134:tid 111134] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Thu Oct 12 07:40:12.126179 2023] [suexec:notice] [pid 111134:tid 111134] AH01232: suEXEC mechanism enabled (wrapper: /u
sr/sbin/suexec)
[Thu Oct 12 07:40:12.144447 2023] [lbmethod_heartbeat:notice] [pid 111134:tid 111134] AH02282: No slotmem from mod_heart
monitor
[Thu Oct 12 07:40:12.155790 2023] [mpm_event:notice] [pid 111134:tid 111134] AH00489: Apache/2.4.53 (Rocky Linux) config
ured -- resuming normal operations
[Thu Oct 12 07:40:12.155889 2023] [core:notice] [pid 111134:tid 111134] AH00094: Command line: '/usr/sbin/httpd -D FOREG
ROUND'
[root@aldoro ~]#
```

Рис. 4.25: `/var/log/httpd/error_log`

```
[root@aldoro ~]# cat /var/log/httpd/access_log
127.0.0.1 - - [12/Oct/2023:07:17:42 +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 - - [12/Oct/2023:07:17:42 +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/20100101 Firefox/115.0"
127.0.0.1 - - [12/Oct/2023:07:26:30 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@aldoro ~]#
```

Рис. 4.26: /var/log/httpd/access_log

```
[root@aldoro ~]# cat /var/log/audit/audit.log
type=DAEMON msg=audit(1697071700.305:9504): op=START ver=3.0.7 format=enriched kernel=5.14.0-284.11.1.el9_2.x86_64
aid=4294967295 pid=712 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1697071700.311:5): pid=1 uid=0 aid=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"
type=CONFIG_CHANGE msg=audit(1697071700.355:6): op=set audit_backlog_limit=8192 old=64 aid=4294967295 ses=4294967295 su
bj=system_u:system_r:unconfined_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1697071700.355:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04fff720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=
sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1697071700.355:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469
742E72756C6573
type=CONFIG_CHANGE msg=audit(1697071700.355:7): op=set audit_failure=1 old=1 aid=4294967295 ses=4294967295 subj=system_
u:system_r:unconfined_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1697071700.355:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04fff720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=
sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1697071700.355:7): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469
742E72756C6573
type=CONFIG_CHANGE msg=audit(1697071700.355:8): op=set audit_backlog_wait_time=60000 old=60000 aid=4294967295 ses=42949
67295 subj=system_u:system_r:unconfined_service_t:s0 res=1AUID="unset"
type=SYSCALL msg=audit(1697071700.355:8): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc04fff720 a2=3c a3=0 i
tems=0 ppid=717 pid=727 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=429496729
5 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=
sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1697071700.355:8): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469
742E72756C6573
```

Рис. 4.27: /var/log/audit/audit.log

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` (рис. 4.28). Добавление порта не производим, т.к. нам известно, что он и так уже добавлен - сразу смотрим список.

Порт 81 есть в списке.

```
[root@aldoro ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@aldoro ~]# semanage port -l |grep http_port_t
bash: semanage: command not found...
[root@aldoro ~]# 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@aldoro ~]#
```

Рис. 4.28: Список портов

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

```

[root@aldoro ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@aldoro ~]# 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 Thu 2023-10-12 07:51:32 MSK; 16s ago
     Docs: man:httpd.service(8)
   Main PID: 111384 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 12221)
   Memory: 22.9M
      CPU: 107ms
   CGroup: /system.slice/httpd.service
           └─111384 /usr/sbin/httpd -DFOREGROUND
             └─111385 /usr/sbin/httpd -DFOREGROUND
               └─111386 /usr/sbin/httpd -DFOREGROUND
                 └─111387 /usr/sbin/httpd -DFOREGROUND
                   └─111388 /usr/sbin/httpd -DFOREGROUND

Oct 12 07:51:32 aldoro.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 12 07:51:32 aldoro.localdomain httpd[111384]: Server configured, listening on: port 81
Oct 12 07:51:32 aldoro.localdomain systemd[1]: Started The Apache HTTP Server.
[root@aldoro ~]#

```

Рис. 4.29: Запуск веб-сервера

Сервер перезапустился также успешно, как и в тот раз, поскольку оба раза порт 81 был в списке портов.

21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html` (рис. 4.30).

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html` (рис. 4.31).

Видим содержимое файла — слово «test».

```

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

```

Рис. 4.30: Возвращаем контекст безопасности

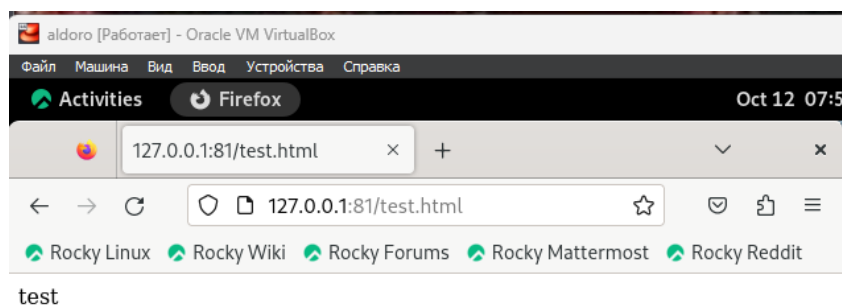


Рис. 4.31: Получение доступа к файлу через веб-сервер

22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80` (рис. 4.32).

```
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
#Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
```

Рис. 4.32: Изменение прослушиваемого порта

23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.

Мы не можем этого сделать, поскольку это была изначальная настройка системы. (рис. 4.33).

24. Удалите файл `/var/www/html/test.html` (рис. 4.33): `rm /var/www/html/test.html`


```
[root@aldoro ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@aldoro ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@aldoro ~]# ls /var/www/html
[root@aldoro ~]#
```

Рис. 4.33: Удаление файла

5 Выводы

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux¹. Проверила работу SELinx на практике совместно с веб-сервером Apache.

Список литературы