

Отчёт по лабораторной работе № 6

Дисциплина: Основы информационной безопасности

Перелыгин Сергей Викторович

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	8
5	Выводы	18
6	Библиография	19

Список иллюстраций

4.1	Проверка режима enforcing политики targeted	8
4.2	Проверка работы веб-сервера	9
4.3	Контекст безопасности веб-сервера Apache	9
4.4	Текущее состояние переключателей SELinux	10
4.5	Статистика по политике	11
4.6	Просмотр файлов и поддиректорий в директории /var/www	11
4.7	Создание файла /var/www/html/test.html	12
4.8	Обращение к файлу через веб-сервер	12
4.9	Изменение контекста	13
4.10	Обращение к файлу через веб-сервер	13
4.11	Установка веб-сервера Apache на прослушивание TCP-порта 81	14
4.12	Содержание файла var/log/http/access_log	14
4.13	Содержание файла var/log/http/error_log	15
4.14	Содержание файла var/log/audit/audit.log	15
4.15	Проверка установки порта 81	16
4.16	Возвращение исходного контекста файлу	16
4.17	Обращение к файлу через веб-сервер	16
4.18	Возвращение Listen 80 и попытка удалить порт 81	17
4.19	Удаление файла test.html	17

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

- Сделать отчёт по лабораторной работе в формате Markdown.
- В качестве отчёта предоставить отчёты в 3 форматах: pdf, docx и md.

3 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. SELinux имеет три основных режим работы:

- Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- Disabled: Полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений(NCSA).

Для чего нужен Apache сервер:


- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,

- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

4 Выполнение лабораторной работы

1. Вошел в систему под своей учетной записью и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus” (рис. 4.1).

A screenshot of a terminal window with a dark background. The window title bar shows a plus icon and the text "sergeiperel@fedora:~". The terminal content shows the execution of two commands: "getenforce" and "sestatus". The output of "getenforce" is "Enforcing". The output of "sestatus" is a multi-line status report.

```
[sergeiperel@fedora ~]$ getenforce
Enforcing
[sergeiperel@fedora ~]$ 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
[sergeiperel@fedora ~]$
```

Рис. 4.1: Проверка режима enforcing политики targeted

2. Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды “service httpd status” (рис. 4.2).


```
sergeiperel@fedora:~ -- /bin/systemctl status httpd.service

[sergeiperel@fedora ~]$ sudo systemctl start httpd
[sudo] пароль для sergeiperel:
[sergeiperel@fedora ~]$ 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:
   Drop-In: /usr/lib/systemd/system/service.d
           └─10-timeout-abort.conf
   Active: active (running) since Sat 2023-10-14 19:19:32 MSK; 11s ago
     Docs: man:httpd.service(8)
  Main PID: 3654 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Byt
  Tasks: 177 (limit: 2296)
   Memory: 19.2M
      CPU: 200ms
   CGroup: /system.slice/httpd.service
           └─3654 /usr/sbin/httpd -DFOREGROUND
             └─3655 /usr/sbin/httpd -DFOREGROUND
               └─3660 /usr/sbin/httpd -DFOREGROUND
                 └─3662 /usr/sbin/httpd -DFOREGROUND
                   └─3663 /usr/sbin/httpd -DFOREGROUND

окт 14 19:19:32 fedora systemd[1]: Starting httpd.service - The Apache HTTP S
окт 14 19:19:32 fedora httpd[3654]: AH00558: httpd: Could not reliably determ
окт 14 19:19:32 fedora systemd[1]: Started httpd.service - The Apache HTTP Sep
окт 14 19:19:32 fedora httpd[3654]: Server configured, listening on: port 80
lines 1-22/22 (END)
```

Рис. 4.2: Проверка работы веб-сервера

3. С помощью команды “ps auxZ | grep httpd” определил контекст безопасности веб-сервера Apache - httpd_t (рис. 4.3).

```
sergeiperel@fedora:~

[sergeiperel@fedora ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3654    0.1  0.5  18744 11552 ?        Ss   19:19   0:00 /usr/sbi
n/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3655    0.0  0.3  18896  7024 ?        S    19:19   0:00 /usr/sbi
n/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3660    0.0  0.4 1109460 8840 ?        Sl   19:19   0:00 /usr/sbi
n/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3662    0.0  0.4  978324  8584 ?        Sl   19:19   0:00 /usr/sbi
n/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3663    0.0  0.4  978324  8712 ?        Sl   19:19   0:00 /usr/sbi
n/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 sergeip+ 3930  0.0  0.1 222436 2432 pts/0 S+  19:21   0
:00 grep --color=auto httpd
[sergeiperel@fedora ~]$
```

Рис. 4.3: Контекст безопасности веб-сервера Apache

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off” (рис. 4.4).



```
r=auto httpd
[sergeiperel@fedora ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.

Without options, show SELinux status.
[sergeiperel@fedora ~]$ 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
```

Рис. 4.4: Текущее состояние переключателей SELinux

5. Посмотрел статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 5116 (рис. 4.5).

```
sergeiperel@fedora:~  
[sergeiperel@fedora ~]$ seinfo  
Statistics for policy file: /sys/fs/selinux/policy  
Policy Version:          33 (MLS enabled)  
Target Policy:           selinux  
Handle unknown classes:  allow  
Classes:                 134    Permissions:          460  
Sensitivities:           1      Categories:           1024  
Types:                   5116   Attributes:            259  
Users:                   8      Roles:                14  
Booleans:                356    Cond. Expr.:          387  
Allow:                   65650   Neverallow:            0  
Auditallow:              171    Dontaudit:             8595  
Type_trans:              266596 Type_change:            87  
Type_member:              35     Range_trans:           6164  
Role allow:              38     Role_trans:            420  
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:                660  
Netifcon:                 0      Nodecon:                0  
[sergeiperel@fedora ~]$
```

Рис. 4.5: Статистика по политике

6. С помощью команды “ls -lZ /var/www” посмотрел файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определил, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 4.6).

```
[sergeiperel@fedora ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 0 map 9 2023 cgi-bin  
drwxr-xr-x. 1 root root system_u:object_r:httpd_sys_content_t:s0 0 map 9 2023 html  
[sergeiperel@fedora ~]$ ls -lZ /var/www/html  
итого 0  
[sergeiperel@fedora ~]$
```

Рис. 4.6: Просмотр файлов и поддиректорий в директории /var/www

7. От имени суперпользователя создал html-файл /var/www/html/test.html. Текст созданного файла - httpd_sys_content_t (рис. 4.7).

```
sergeiperel@fedora:~  
[sergeiperel@fedora ~]$ su -  
Пароль:  
su: Сбой при проверке подлинности  
[sergeiperel@fedora ~]$ sudo su -  
[root@fedora ~]# touch /var/www/html/test.html  
[root@fedora ~]# emacs test.html&  
[1] 5412  
[root@fedora ~]#  
[1]+  Завершён          emacs test.html  
[root@fedora ~]# cat /var/www/html/test.html  
[root@fedora ~]# nano /var/www/html/test.html  
[root@fedora ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@fedora ~]# exit  
ВЫХОД  
[sergeiperel@fedora ~]$
```

Рис. 4.7: Создание файла /var/www/html/test.html

8. Обратился к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”.
Файл был успешно отображен (рис. 4.8).

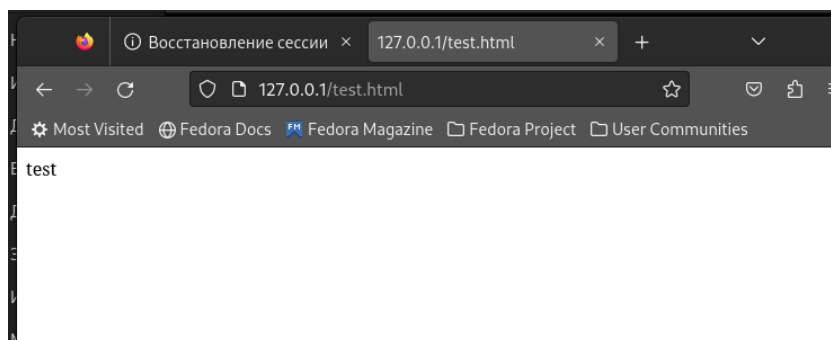
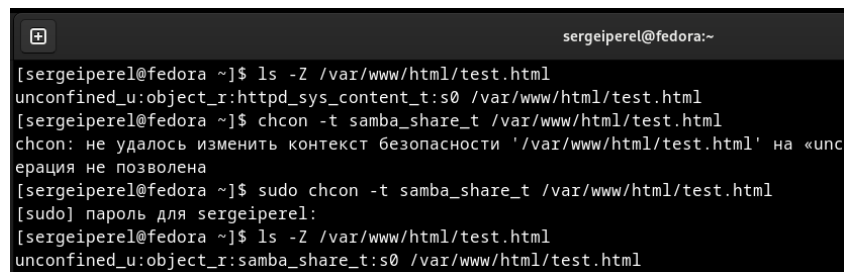


Рис. 4.8: Обращение к файлу через веб-сервер

9. Изучив справку `man httpd_selinux`, выяснил, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`. Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменил контекст файла на `samba_share_t` командой

“sudo chcon -t samba_share_t /var/www/html/test.html” и проверил, что контекст поменялся (рис. 4.9).



```
sergeiperel@fedora:~  
[sergeiperel@fedora ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[sergeiperel@fedora ~]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unc  
ерация не позволена  
[sergeiperel@fedora ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
[sudo] пароль для sergeiperel:  
[sergeiperel@fedora ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 4.9: Изменение контекста

10. Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получил сообщение об ошибке (т.к. к установленному ранее контексту процесс httpd не имеет доступа) (рис. 4.10).

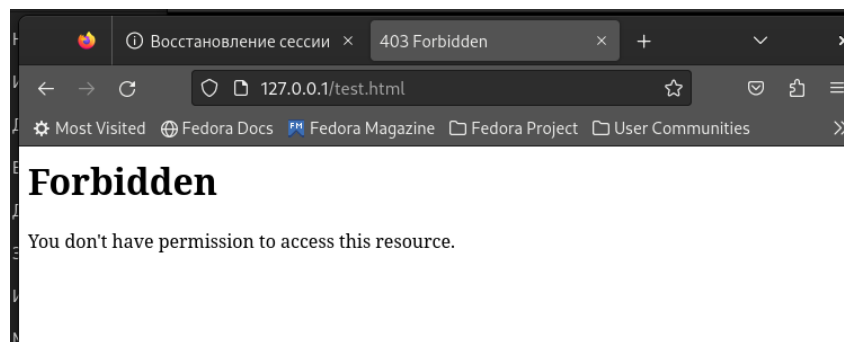


Рис. 4.10: Обращение к файлу через веб-сервер

11. Командой “ls -l /var/www/html/test.html” убедился, что читать данный файл может любой пользователь. Просмотрел системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки.
12. В файле /etc/httpd/conf/httpd.conf заменил строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 4.11).

```
root@fedora:~  
GNU nano 7.2 /etc/httpd/conf/httpd.conf  
  
#  
# ServerRoot: The top of the directory tree under which the server's  
# configuration, error, and log files are kept.  
#  
# Do not add a slash at the end of the directory path. If you point  
# ServerRoot at a non-local disk, be sure to specify a local disk on the  
# Mutex directive, if file-based mutexes are used. If you wish to share the  
# same ServerRoot for multiple httpd daemons, you will need to change at  
# least PidFile.  
#  
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 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 81  
  
#  
# Dynamic Shared Object (DSO) Support  
#  
# To be able to use the functionality of a module which was built as a DSO you
```

^G Справка	^O Записать	^W Поиск	^K Вырезать	^T Выполнить	^C Позиция
^X Выход	^R ЧитФайл	^_ Замена	^U Вставить	^J Выворнять	^/_ К строке

Рис. 4.11: Установка веб-сервера Apache на прослушивание TCP-порта 81

13. Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -nl /var/log/messages”.
14. Просмотрел файлы “var/log/http/error_log”, “/var/log/http/access_log” и “/var/log/audit/audit.log” и выяснил, что запись появилась в последнем файле (рис. 4.12 - 4.14).

```
[root@fedora logs]# cat access_log  
127.0.0.1 - - [14/Oct/2023:19:48:50 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0 Gecko/20100101 Firefox/111.0)"  
127.0.0.1 - - [14/Oct/2023:19:48:52 +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/111.0"  
127.0.0.1 - - [14/Oct/2023:19:52:19 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0 Gecko/20100101 Firefox/111.0)"  
[root@fedora logs]# cat error_log
```

Рис. 4.12: Содержание файла var/log/http/access_log

```
[root@fedora logs]# cat error_log
[Sat Oct 14 19:19:32.278524 2023] [suexec:notice] [pid 3654:tid 3654] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::4d55:e9c7:e43a:9ed4%eth0:3. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 14 19:19:32.313148 2023] [lbmethod_heartbeat:notice] [pid 3654:tid 3654] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 19:19:32.316344 2023] [systemd:notice] [pid 3654:tid 3654] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 19:19:32.378267 2023] [.:warn] [pid 3656:tid 3656] ./mod_dnssd.c: No services found to register
[Sat Oct 14 19:19:32.380807 2023] [mpm_event:notice] [pid 3654:tid 3654] AH00489: Apache/2.4.56 (Fedora Linux) configured -- resuming normal operations
[Sat Oct 14 19:19:32.380837 2023] [core:notice] [pid 3654:tid 3654] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4.13: Содержание файла var/log/http/error_log

```
root@fedora:/var/log/audit
type=USER_CMD msg=audit(1697303852.262:784): pid=8217 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="cwd="/etc/httpd" cmd="7375202D" exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="sergeiperel" sergeiperel"
type=CRED_REFR msg=audit(1697303852.263:785): pid=8217 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sergeiperel" AUID="sergeiperel"
type=USER_START msg=audit(1697303852.271:786): pid=8217 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_uacct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sergeiperel" AUID="sergeiperel"
type=USER_AUTH msg=audit(1697303852.302:787): pid=8218 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:authentication grantors=pam_rootok acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/pts/0 res=success'UID="root" AUID="sergeiperel"
type=USER_ACCT msg=audit(1697303852.303:788): pid=8218 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:accounting grantors=pam_succeed_if acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/pts/0 res=success'UID="root" AUID="sergeiperel"
type=CRED_ACQ msg=audit(1697303852.306:789): pid=8218 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:setcred grantors=pam_rootok acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="root" AUID="sergeiperel"
type=USER_START msg=audit(1697303852.370:790): pid=8218 uid=0 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg="op=PAM:session_open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,th acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="root" AUID="sergeiperel"
type=BPF msg=audit(1697303852.436:791): prog-id=114 op=LOAD
type=BPF msg=audit(1697303852.437:792): prog-id=115 op=LOAD
type=BPF msg=audit(1697303852.441:793): prog-id=116 op=LOAD
type=SERVICE_START msg=audit(1697303852.581:794): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:systemd:unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1697303882.635:795): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:systemd:unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1697303882.647:796): prog-id=116 op=UNLOAD
type=BPF msg=audit(1697303882.647:797): prog-id=115 op=UNLOAD
type=BPF msg=audit(1697303882.647:798): prog-id=114 op=UNLOAD
[root@fedora audit]#
```

Рис. 4.14: Содержание файла var/log/audit/audit.log

15. Выполнил команду “semanage port -a -t http_port_t -p tcp 81” и убедился, что порт TCP-81 установлен. Проверил список портов командой “semanage port -l | grep http_port_t”, убедился, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 4.15).

```

[root@fedora audit]# cd ~
[root@fedora ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,mo
               ...
semanage: error: unrecognized arguments: -p 81
[root@fedora ~]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443,
pegasus_http_port_t tcp      5988
[root@fedora ~]# systemctl restart httpd
[root@fedora ~]#

```

Рис. 4.15: Проверка установки порта 81

16. Вернул контекст “httpd_sys_content_t” файлу “/var/www/html/test.html” командой “chcon -t httpd_sys_content_t /var/www/html/test.html” (рис. 4.16) и после этого попробовал получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидел содержимое файла - слово “test” (рис. 4.17).

```

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

```

Рис. 4.16: Возвращение исходного контекста файлу

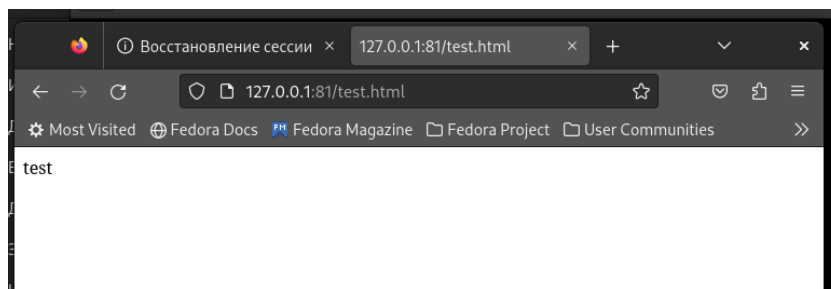
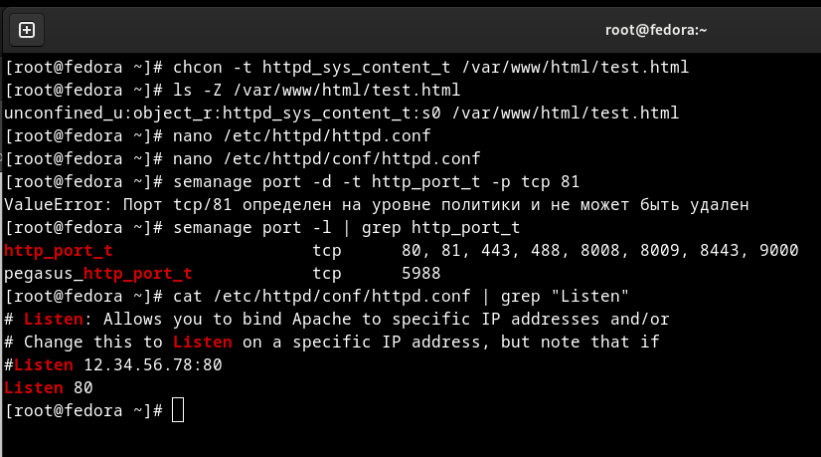


Рис. 4.17: Обращение к файлу через веб-сервер

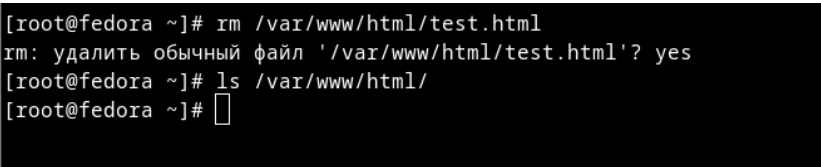
17. Исправил обратно конфигурационный файл apache, вернув “Listen 80”. Попытался удалить привязку http_port к 81 порту командой “semanage port -d -t http_port_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить (рис. 4.18).



```
root@fedora:~  
[root@fedora ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@fedora ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@fedora ~]# nano /etc/httpd/httpd.conf  
[root@fedora ~]# nano /etc/httpd/conf/httpd.conf  
[root@fedora ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[root@fedora ~]# 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@fedora ~]# cat /etc/httpd/conf/httpd.conf | grep "Listen"  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# Change this to Listen on a specific IP address, but note that if  
#Listen 12.34.56.78:80  
Listen 80  
[root@fedora ~]#
```

Рис. 4.18: Возвращение Listen 80 и попытка удалить порт 81

18. Удалил файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 4.19).



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

Рис. 4.19: Удаление файла test.html

5 Выводы

Вывод: В ходе выполнения данной лабораторной работы я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux и проверил работу SELinux на практике совместно с веб-сервером Apache.

6 Библиография

- Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
- Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
- Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.
- Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)