

Отчет по лабораторной работе №6

Информационная безопасность

Коломиец Мария Владимировна НПИбд-01-18

Содержание

1 Цель работы	4
2 Теоретическое описание	5
3 Подготовка лабораторного стенда:	6
4 Выполнение лабораторной работы	8
5 Выводы	19

Список иллюстраций

3.1 Параметр ServerName	6
3.2 Отключение фильтра	7
3.3 Добавление разрешающих правил	7
4.1 Проверка	8
4.2 Обращение через браузер	9
4.3 Проверка	9
4.4 веб-сервер Apache	10
4.5 Просмотр состояния переключателей SELinux для Apache	10
4.6 Получение информации	11
4.7 Создание файла	12
4.8 Проверка	12
4.9 Получение доступа к файлу через браузер	13
4.10 Проверка контекста	13
4.11 Изменение контекста, проверка	13
4.12 Получение доступа к файлу через браузер	14
4.13 Проверка	14
4.14 Просмотр системного лог-файла	14
4.15 Просмотр системного лог-файла	15
4.16 Изменение порта 80 на 81	15
4.17 Анализ лог-файла	15
4.18 Просмотр файла /var/log/http/error_log	16
4.19 Просмотр файла /var/log/http/access_log	16
4.20 Просмотр файла var/log/audit/audit.log	16
4.21 Выполнение и проверка	17
4.22 Возвращение контекста	17
4.23 Получение доступа к файлу через браузер	17
4.24 Исправление конфигурационного файла apache	18
4.25 Удаление привязки http_port_t к 81 порту	18
4.26 Удаление файла /var/www/html/test.html	18

1 Цель работы

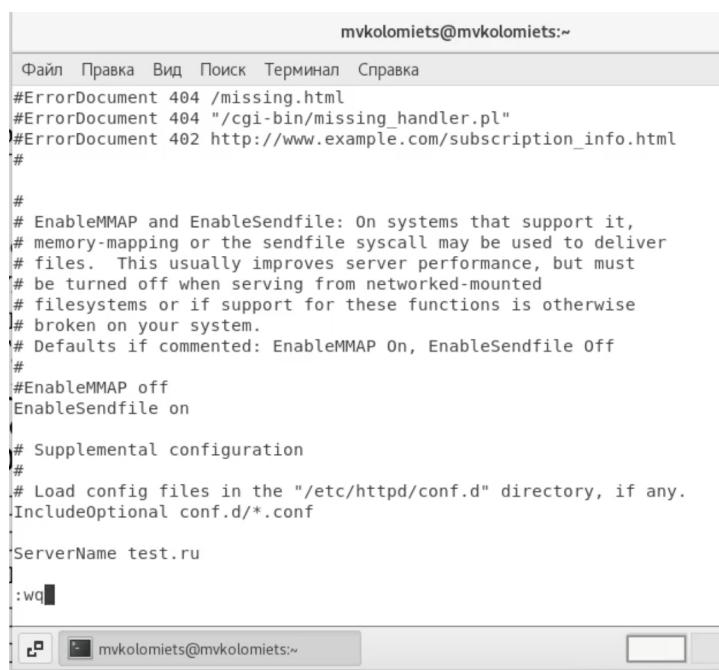
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Теоретическое описание

SELinux — набор технологий расширения системы безопасности Linux. Сегодня основу набора составляют три технологии: мандатный контроль доступа, ролевой доступ RBAC и система типов (доменов). 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.

3 Подготовка лабораторного стенда:

1. В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName. (рис. 3.1).



The screenshot shows a terminal window with the title bar "mvkolomiets@mvkolomiets:~". The window contains the following text:

```
mvkolomiets@mvkolomiets:~  
Файл Правка Вид Поиск Терминал Справка  
#ErrorDocument 404 /missing.html  
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"  
#ErrorDocument 402 http://www.example.com/subscription_info.html  
#  
#  
# EnableMMAP and EnableSendfile: On systems that support it,  
# memory-mapping or the sendfile syscall may be used to deliver  
# files. This usually improves server performance, but must  
# be turned off when serving from networked-mounted  
# filesystems or if support for these functions is otherwise  
# broken on your system.  
# Defaults if commented: EnableMMAP On, EnableSendfile Off  
#  
#EnableMMAP off  
EnableSendfile on  
  
# Supplemental configuration  
#  
# Load config files in the "/etc/httpd/conf.d" directory, if any.  
IncludeOptional conf.d/*.conf  
  
ServerName test.ru  
:  
:wq
```

The terminal window has a standard Linux-style interface with tabs for "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar at the bottom shows the user name "mvkolomiets" and the host name "mvkolomiets:~".

Рис. 3.1: Параметр ServerName

2. Также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавила разрешающие правила. (рис. 3.2), (рис. 3.3).

```
[root@mvmkolomiets ~]# iptables -F  
[root@mvmkolomiets ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```

Рис. 3.2: Отключение фильтра

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

Рис. 3.3: Добавление разрешающих правил

4 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.(рис. 4.1).

```
[root@mvkolomiets ~]# getenforce
Enforcing
[root@mvkolomiets ~]# 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
Max kernel policy version:      31
[root@mvkolomiets ~]# █
```

Рис. 4.1: Проверка

2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: service httpd status(рис. 4.2), (рис. 4.3).

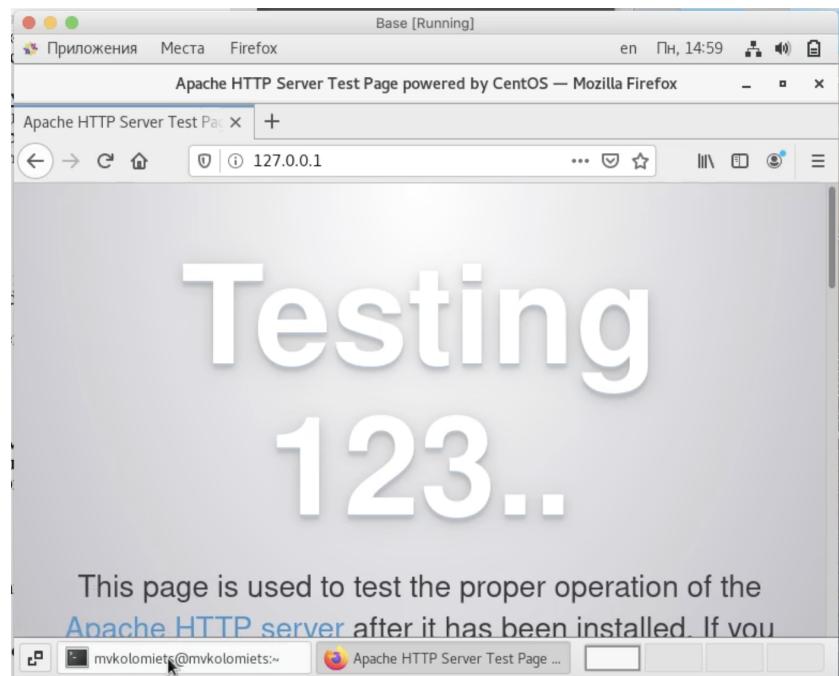


Рис. 4.2: Обращение через браузер

```
[root@mvkolumets ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@mvkolumets ~]# 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; vendor preset: disabled)
      Active: active (running) since Пн 2021-11-22 14:58:36 MSK; 2s ago
        Docs: man:httpd(8)
               man:apachectl(8)
    Main PID: 3743 (httpd)
      Status: "Processing requests..."
         Tasks: 6
        CGroup: /system.slice/httpd.service
                  ├─3743 /usr/sbin/httpd -DFOREGROUND
                  ├─3748 /usr/sbin/httpd -DFOREGROUND
                  ├─3749 /usr/sbin/httpd -DFOREGROUND
                  ├─3750 /usr/sbin/httpd -DFOREGROUND
                  ├─3751 /usr/sbin/httpd -DFOREGROUND
                  └─3752 /usr/sbin/httpd -DFOREGROUND

ноя 22 14:58:36 mvkolumets.localdomain systemd[1]: Starting The Apache HTTP S...
ноя 22 14:58:36 mvkolumets.localdomain systemd[1]: Started The Apache HTTP Se...
Hint: Some lines were ellipsized, use -l to show in full.
[root@mvkolumets ~]#
```

Рис. 4.3: Проверка

3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. (рис. 4.4).

```
[root@mvkolomiets ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3743  0.0  0.4 224084  5048 ?        Ss
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3749  0.0  0.3 226304  3832 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3750  0.0  0.3 226304  3800 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3751  0.0  0.3 226304  3832 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3752  0.0  0.3 226304  3832 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3820  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3821  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3822  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3823  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s?    apache    3824  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3825  0.0  0.3 226168  3096 ?        S
14:58  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3835 0.0  0.0 112832 976
pts/0 R+ 14:59  0:00 grep --color=auto httpd
[root@mvkolomiets ~]#
```

Рис. 4.4: веб-сервер Apache

- Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -b`
grep httpd. Обратила внимание, что многие из них находятся в положении «off». (рис. 4.5).

```
[root@mvkolomiets ~]# 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
Max kernel policy version:     31

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
```

Рис. 4.5: Просмотр состояния переключателей SELinux для Apache

5. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей(8), ролей(14), типов(4793). Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 4.6).

```
[root@mvkolomiets ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130    Permissions:      272
Sensitivities:     1    Categories:      1024
Types:           4793    Attributes:       253
Users:            8    Roles:             14
Booleans:         316    Cond. Expr.:    362
Allow:          107834    Neverallow:      0
Auditallow:        158    Dontaudit:     10022
Type_trans:       18153    Type_change:    74
Type_member:        35    Role allow:    37
Role_trans:        414    Range_trans:   5899
Constraints:       143    Validatetrans:  0
Initial SIDs:       27    Fs_use:         32
Genfscon:          103    Portcon:       614
Netifcon:            0    Nodecon:        0
Permissives:        0    Polcap:         5

[root@mvkolomiets ~]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@mvkolomiets ~]# ls -lZ /var/www/html
[root@mvkolomiets ~]# ls /var/www
cgi-bin  html
[root@mvkolomiets ~]#
```

Рис. 4.6: Получение информации

6. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 4.7).

Рис. 4.7: Создание файла

7. Проверила контекст созданного файла. httpd_sys_content_t (рис. 4.8).

```
[root@mvkolomiets ~]# vi /var/www/html/test.html
[root@mvkolomiets ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@mvkolomiets ~]#
```

Рис. 4.8: Проверка

8. Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён. (рис. 4.9).

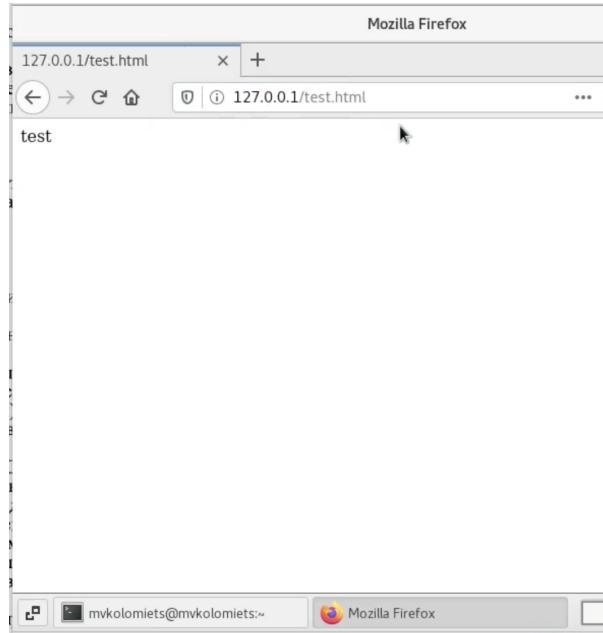


Рис. 4.9: Получение доступа к файлу через браузер

9. Проверила контекст файла командой: ls -Z /var/www/html/test.html (рис. 4.10).

```
[root@mvkolomiets ~]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 4.10: Проверка контекста

10. Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t. После этого проверила, что контекст поменялся. (рис. 4.11).

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

Рис. 4.11: Изменение контекста, проверка

11. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получили сообщение об ошибке. (рис. 4.12).

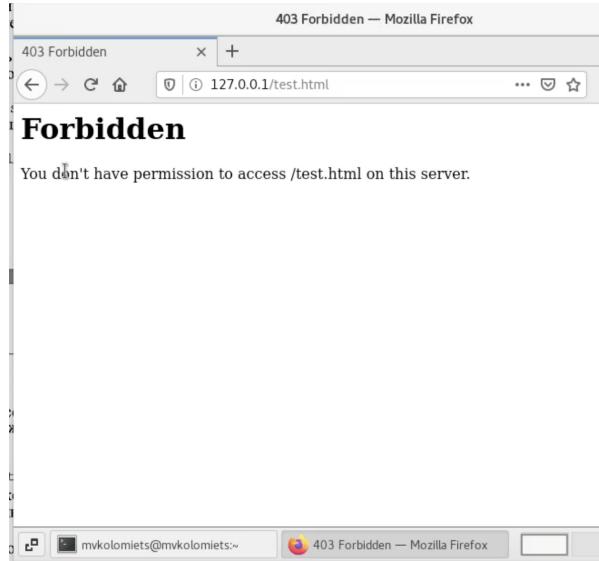


Рис. 4.12: Получение доступа к файлу через браузер

12. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages (рис. 4.13), (рис. 4.14), (рис. 4.15).

```
[root@mvkoloimiets ~]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 Nov 22 15:06 /var/www/html/test.html  
[root@mvkoloimiets ~]#
```

Рис. 4.13: Проверка

```
[root@mvkmolniets ~]# tail /var/log/messages
Aug 22 15:12:22 mvkmolniets scribusreouthost: failed to retrieve rpm info for /var/www/html/test.html
Aug 22 15:12:22 mvkmolniets scribusreouthost: SELinux is preventing httpd from getattr a
ccess on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l aae94abaf-e0fd-4683-b538-47978d7db879
[Nov 22 15:12:22 mvkmolniets python]: SELinux is preventing httpd from getattr access on
the file /var/www/html/test.html. #012#012**** Plugin restorecon (92.2 confidence) s
uggests *****#012#012if you want to fix the label. #012#var/www/html/test.html default
label should be httpd sys_content_t. #012#then you can run restore
con. The access attempt may have been stopped due to insufficient permissions to acces
s a parent directory in which case try to change the following command accordingly. #01
#020#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public conte
nt_t (7.83 confidence) suggests *****#012#012if you want to treat test.
html as public content#012#then you need to change the label on test.html to public con
tent_t or public content_rv_t. #012#012# semanage fcontext -a -t public_content_t '/
var/www/html/test.html' #012# restorecon -v '/var/www/html/test.html'#012#012**** Plug
in catchall (1.41 confidence) suggests *****#012#012if you beli
eve that httpd should be allowed getattr access on the test.html file by default. #012#
then you should add the rule. #012#You can generate a local policy module to allo
w this via semanage fcontext -a -t httpd_sys_content_t '/var/www/html/test.html' #012#
allow this access for now by executing #012#ausearch -c 'http
d' -r -l | auditallow -M my_httpd #012# semodule -i my_httpd.pp#012
Nov 22 15:14:23 mvkmolniets dbus[692]: [system] Activating service=org.freedesk
op.problems" (using servicehelper)
Nov 22 15:14:23 mvkmolniets dbus[692]: [system] Successfully activated service 'org.fr
```

Рис. 4.14: Просмотр системного лог-файла

```

Suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. 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 public content#012#Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012#012# semanage 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 allowed gettattr access on the test.html file by default.#012# then you should report this as a bug.#012# You can generate a local policy module to allow this access:#012#audit2allow -F my-httdp -m my-httdp.pp#012 Nov 22 15:14:23 mvkolomiets dbus[692]: [system] Activating service name='org.freedesktop.problems' (using servicehelper)
Nov 22 15:14:23 mvkolomiets dbus[692]: [system] Successfully activated service 'org.freedesktop.problems'
Nov 22 15:14:26 mvkolomiets dbus[692]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Nov 22 15:14:26 mvkolomiets systemd: Starting Fingerprint Authentication Daemon...
Nov 22 15:14:26 mvkolomiets dbus[692]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 22 15:14:26 mvkolomiets systemd: Started Fingerprint Authentication Daemon.
Nov 22 15:14:29 mvkolomiets su: (to root) mvkolomiets on pts/1
[root@mvkolomiets ~]#

```

Рис. 4.15: Просмотр системного лог-файла

13. Попробовала 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 нашла строчку Listen 80 и заменил её на Listen 81.(рис. 4.16).

```

mvkolomiets@mvkolomiets:~# vim /etc/httpd/conf.d/httpd.conf
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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
# 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.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
-- INSERT --

```

Рис. 4.16: Изменение порта 80 на 81

14. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (рис. 4.17), (рис. 4.18), (рис. 4.19), (рис. 4.20).

```

[root@mvkolomiets ~]# tail -n1 /var/log/messages
Nov 22 15:20:01 mvkolomiets systemd: Removed slice User Slice of root.
[root@mvkolomiets ~]#

```

Рис. 4.17: Анализ лог-файла

```
[root@mvkolumiets ~]# cat /var/log/httpd/error_log
[Mon Nov 22 14:58:36.877577 2021] [core:notice] [pid 3743] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Mon Nov 22 14:58:36.880078 2021] [suexec:notice] [pid 3743] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Mon Nov 22 14:58:36.889424 2021] [lbbmethod_heartbeat:notice] [pid 3743] AH02282: No slotmem from mod_heartmonitor
[Mon Nov 22 14:58:36.891952 2021] [mpm_prefork:notice] [pid 3743] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Mon Nov 22 14:58:36.892071 2021] [core:notice] [pid 3743] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Mon Nov 22 14:58:36.756214 2021] [autoindex:error] [pid 3750] [client 127.0.0.1:43946] AH01276: Cannot serve directory /var/www/html/: No matching DirectoryIndex (index.html) found, and server-generated directory index forbidden by Options directive
[Mon Nov 22 15:18:34.754571 2021] [core:error] [pid 3823] (13)Permission denied: [client 127.0.0.1:43994] AH01270: child could not create socket '/var/www/html/test.html' because search permissions are missing on a component of the path
[Mon Nov 22 15:18:33.607679 2021] [mpm_prefork:notice] [pid 3743] AH00170: caught SIGWINCH, shutting down gracefully
[Mon Nov 22 15:18:34.696286 2021] [core:notice] [pid 4487] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Mon Nov 22 15:18:34.698186 2021] [suexec:notice] [pid 4487] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Mon Nov 22 15:18:34.706968 2021] [lbbmethod_heartbeat:notice] [pid 4487] AH02282: No slotmem from mod_heartmonitor
[Mon Nov 22 15:18:34.708539 2021] [mpm_prefork:notice] [pid 4487] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Mon Nov 22 15:18:34.708539 2021] [core:notice] [pid 4487] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 4.18: Просмотр файла /var/log/http/error_log

```
[root@mvkolumiets ~]# cat /var/log/httpd/access_log
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET / HTTP/1.1" 403 4897 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /noindex/css/bootstrap.min.css HTTP/1.1" 200 19341 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /noindex/css/open-sans.css HTTP/1.1" 200 5081 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /images/apache_pb.gif HTTP/1.1" 200 23 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /images/poweredby.png HTTP/1.1" 200 39 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /noindex/css/fonts/Light/OpenSans-Light.woff HTTP/1.1" 404 238 "http://127.0.0.1/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /noindex/css/fonts/Bold/OpenSans-Bold.woff HTTP/1.1" 404 238 "http://127.0.0.1/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [22/Nov/2021:14:58:58 +0300] "GET /noindex/css/fonts/Light/OpenSans-Light.ttf HTTP/1.1" 404 240 "http://127.0.0.1/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Рис. 4.19: Просмотр файла /var/log/http/access_log

```
[root@mvkolumiets mvkolumiets:~]# cat /var/log/audit/audit.log
bad notice (seqno=3) exeq="/usr/bin/dbus-daemon" sauid=81 hostname=? addr=? terminal=? type=USER MAC CONFIG_CHANGE msg=audit(1634643917.145:149): pid=1569 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:unconfined service t:s0 mspl="resrcfcntext op=modify tglob=/usr/bin/VBoxClient" ftype=any tcontext=system u:object r:unconfined execname exec:t:s0 comm="semanage" exe="/usr/bin/python2.7" hostname=? addr=? terminal=? res=success'
type=SERVICE START msg=audit(1634643917.229:150): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="unit=vboxadd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE START msg=audit(1634643917.305:151): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="unit=gdm comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE START msg=audit(1634643917.310:152): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="unit=vboxadd-service comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SYSTEM RUNLEVEL msg=audit(1634643917.328:153): pid=1604 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="old-level= new-level=5 comm="systemd-update-utmp" exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success'
type=SYSTEM RUNLEVEL msg=audit(1634643917.333:154): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="unit=systemd-update-utmp,rule=0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SYSTEM STOP msg=audit(1634643917.333:155): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system u:system r:init t:s0 mspl="unit=systemd-update-utmp,rule=0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=USER AUTH msg=audit(1634643920.421:156): pid=1627 uid=0 auid=4294967295 ses=4294967295
```

Рис. 4.20: Просмотр файла var/log/audit/audit.log

15. Выполнила команду: semanage port -a -t http_port_t -p tcp 81. После этого проверила список портов командой: semanage port -l | grep http_port_t. Убедилась, что порт 81 появился в списке. (рис. 4.21).

```
[root@mvkolumets ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@mvkolumets ~]# 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@mvkolumets ~]#
```

Рис. 4.21: Выполнение и проверка

16. Вернула контекст httpd_sys_content_t к файлу /var/www/html/test.html: chcon -t httpd_sys_content_t /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидели содержимое файла — слово «test». (рис. 4.22), (рис. 4.23).

```
[root@mvkolumets ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mvkolumets ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 22 15:06 /var/www/html/test.html
[root@mvkolumets ~]# ls -Z /var/www/html/test.html
:rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@mvkolumets ~]#
```

Рис. 4.22: Возвращение контекста

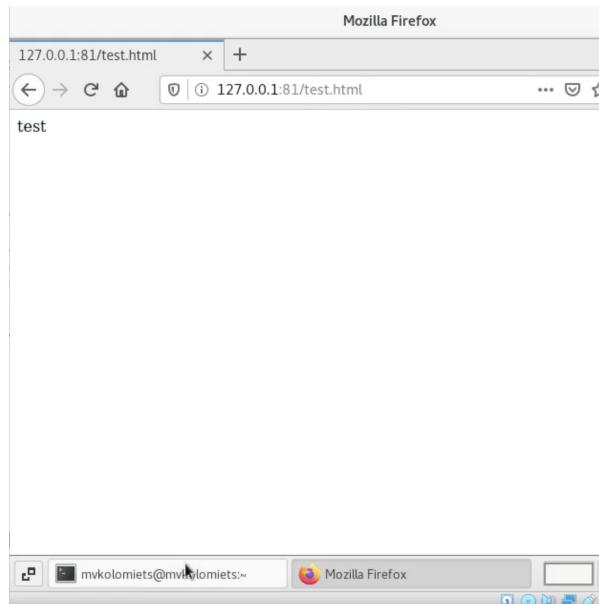
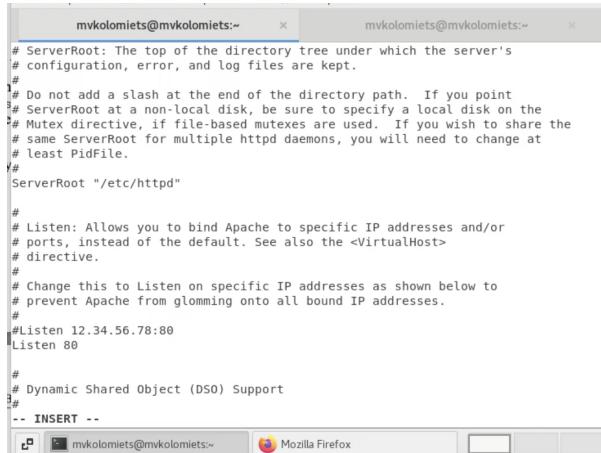


Рис. 4.23: Получение доступа к файлу через браузер

17. Исправила обратно конфигурационный файл apache, вернув Listen80. (рис. 4.24).



```
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
-- INSERT --
```

Рис. 4.24: Исправление конфигурационного файла apache

18. Удалила привязку http_port_t к 81 порту. (рис. 4.25).

```
[root@mvkolumets ~]# semanage port -d -t http_port_t -p tcp 81
```

Рис. 4.25: Удаление привязки http_port_t к 81 порту

19. Удалила файл /var/www/html/test.html. (рис. 4.26).

```
[root@mvkolumets ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@mvkolumets ~]#
```

Рис. 4.26: Удаление файла /var/www/html/test.html

5 Выводы

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.