Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Миличевич Александра

Содержание

Список таблиц

Список иллюстраций

Цель работы

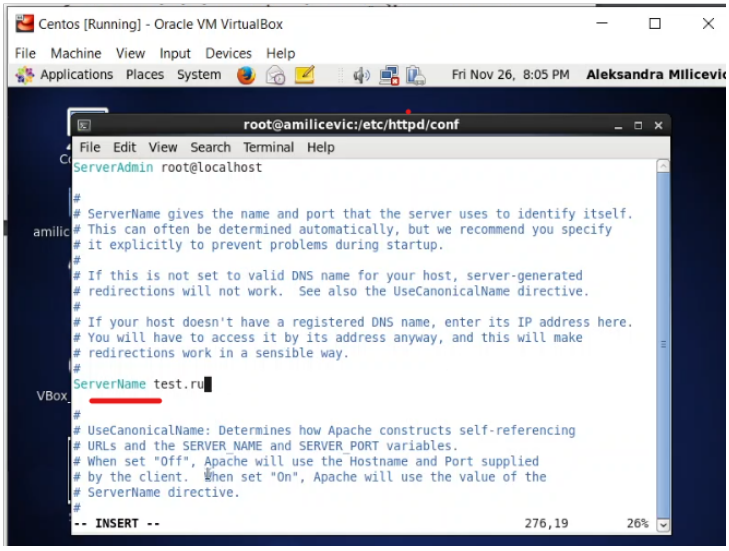
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1 Проверить работу SELinx на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

**Последовательность выполнения работы*

1. 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

В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName.



Отключила фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавила разрешающие правила.

```
root@amilicevic ~]# iptables -F
root@amilicevic ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
ad argument `iptables'
ry `iptables -h' or 'iptables --help' for more information.
root@amilicevic ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
root@amilicevic ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
root@amilicevic ~]# iptables -I OUTPUT -p tcp --dport 80 -j ACCEPT
root@amilicevic ~]# iptables -I OUTPUT -p tcp --dport 81 -j ACCEPT
```

Рис. 0.1: Рис. 2.

2. Вход в систему Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus

```
[root@amilicevic ~]# getenforce
Enforcing
[root@amilicevic ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
[root@amilicevic ~]#
```

Рис. 0.2: Рис. 3.

Обратилась с помощью браузера к веб-серверу, запущенному на компьютере

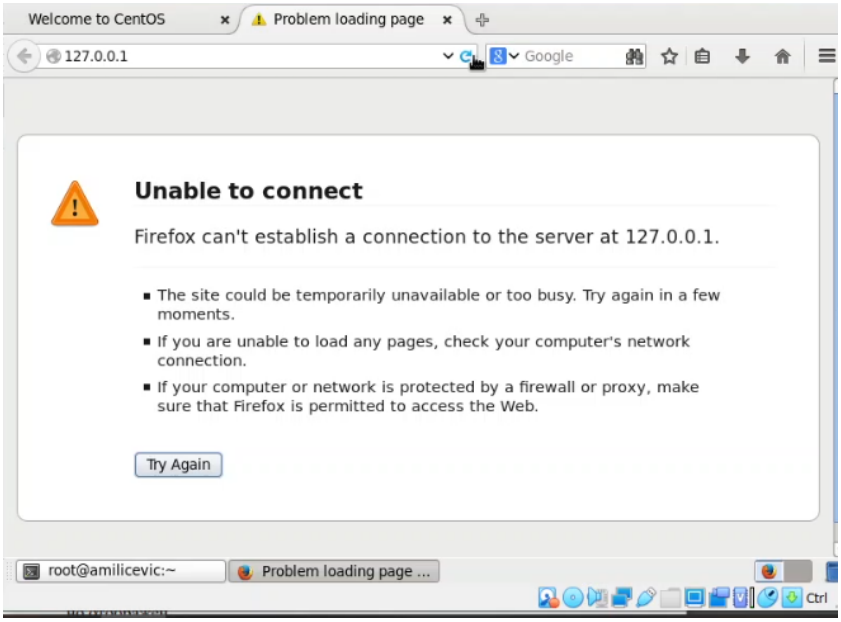


Рис. 0.3: Рис. 4.

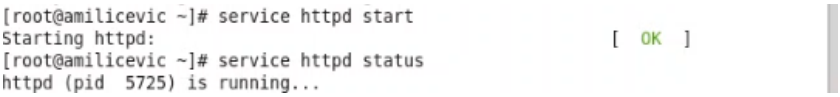
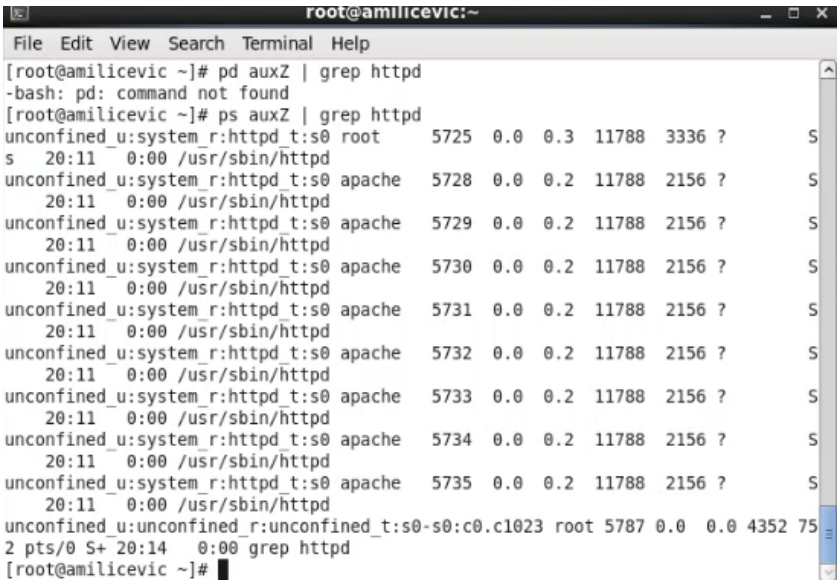


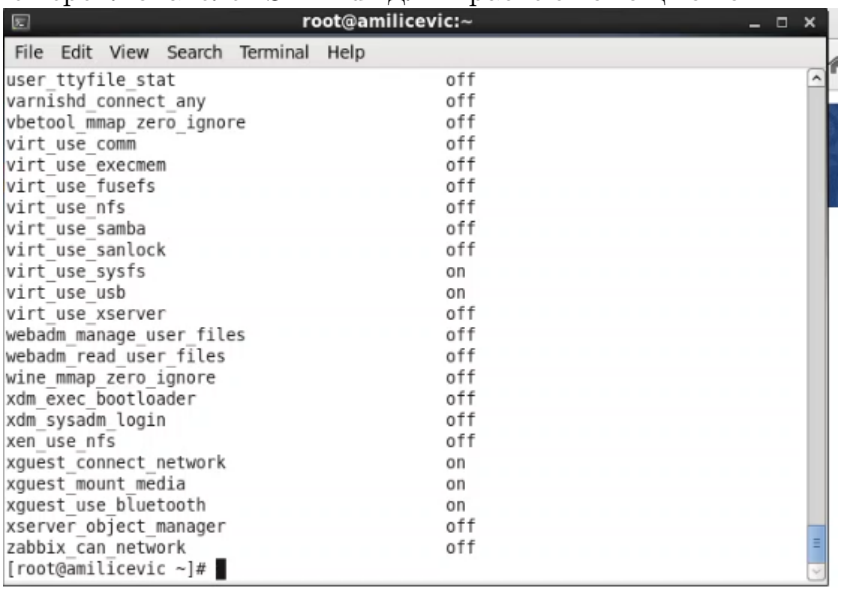
Рис. 0.4: Рис. 5.

3. веб-сервер Apache Нашла веб-сервер Apache в списке процессов, определила его



контекст безопасности.

Посмотрела текущее состояние переключателей SELinux для Apache с помощью ко-



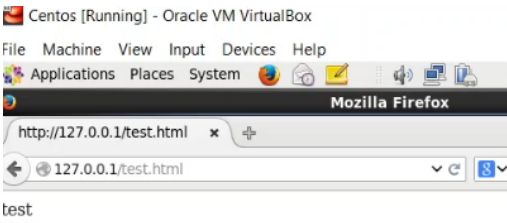
манды: **sestatus -bigrep httpd.

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. 0.5: Рис. 8.

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

Рис. 0.6: Рис. 9.



Проверила контекст созданного файла. httpd_sys_content_t

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. файл был успешно отображён

```
[root@amilicevic html]# ls -lZ /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. 0.7: Рис. 11.

Проверила контекст файла командой: ls -Z /var/www/html/test.html Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t. После этого проверила, что контекст поменялся. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение failiure.

```
[root@amilicevic html]# cd
[root@amilicevic ~]# chcon -t samba_share_t /var/www/html/test.html
[root@amilicevic ~]# 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@amilicevic ~]#
```

Рис. 0.8: Рис. 12.

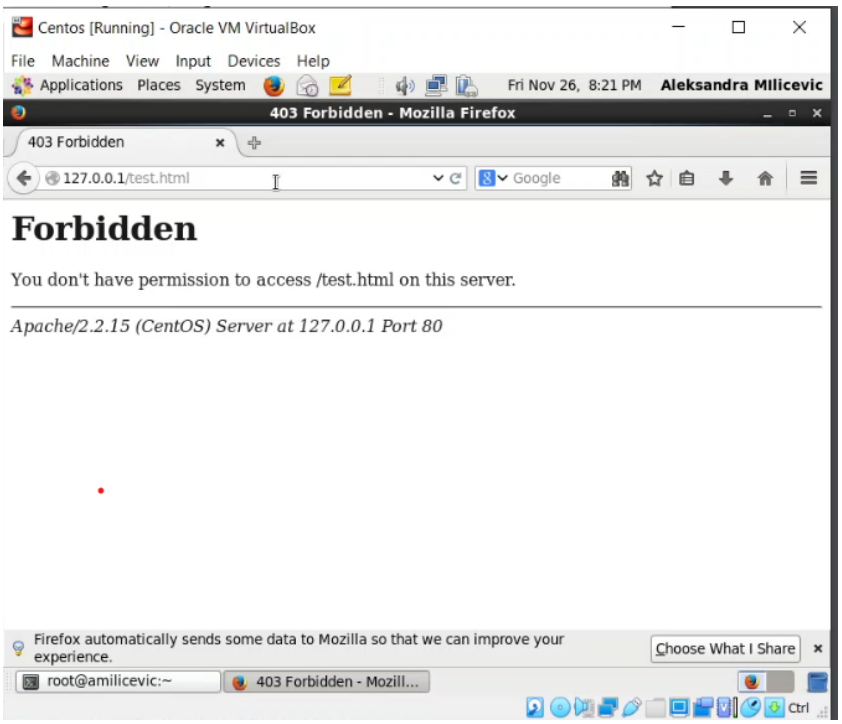


Рис. 0.9: Рис. 13.

Рис. 0.10: Рис. 14.

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. 0.11: Рис. 16.

в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и замените её на Listen 81. Проанализиировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (рис.18), (рис. 4.19), (рис.(рис. 20)

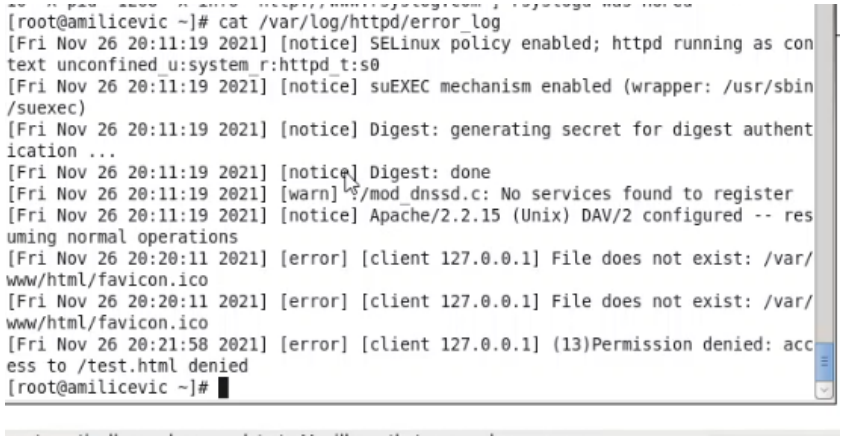
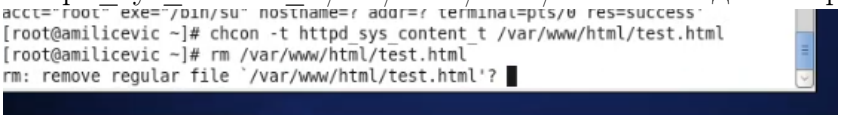


Рис. 0.12: Рис. 17.

Вернула контекст httpd_sys_content__t к файлу /var/www/html/test.html: chcon -t httpd_sys_content_t /var/www/html/test.html. Удалила файл /var/www/html/test.html



Выводы

Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.