

# Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Миличевич Александра

# Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	14

## Список таблиц

# Список иллюстраций

0.1	Рис. 2.	7
0.2	Рис. 3.	7
0.3	Рис. 4.	8
0.4	Рис. 5.	8
0.5	Рис. 8.	10
0.6	Рис. 9.	10
0.7	Рис. 11.	11
0.8	Рис. 12.	11
0.9	Рис. 13.	12
0.10	Рис. 14.	12
0.11	Рис. 16.	13
0.12	Рис. 17.	13

## Цель работы

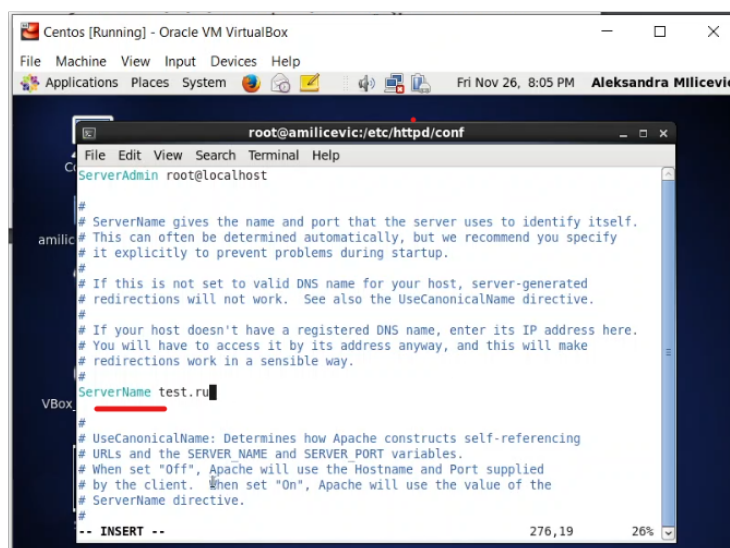
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup> Проверить работу SELinx на практике совместно с веб-сервером Apache.

# 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` задали 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

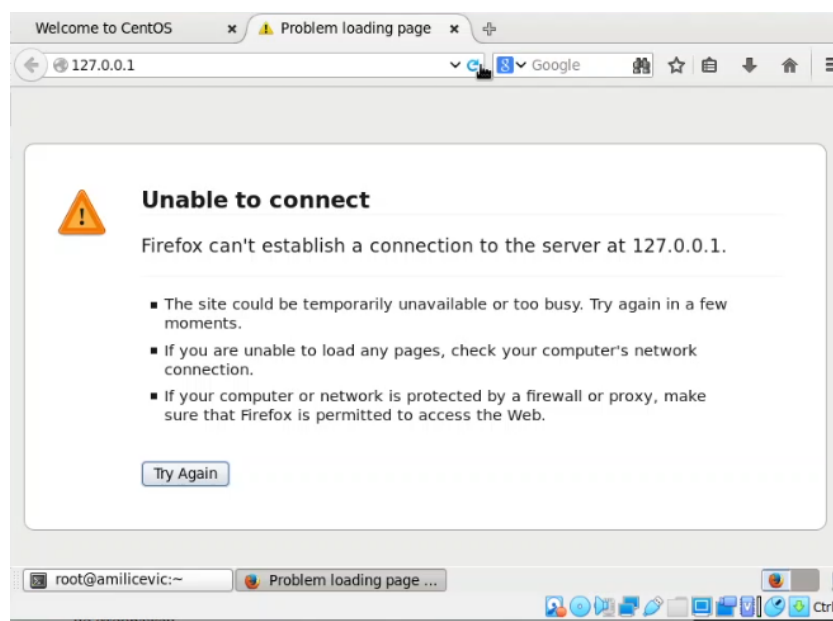


Рис. 0.3: Рис. 4.

```
[root@amilicevic ~]# service httpd start
Starting httpd:
[root@amilicevic ~]# service httpd status
httpd (pid 5725) is running... [ OK ]
```

Рис. 0.4: Рис. 5.

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



```
root@amilicevic:~  
File Edit View Search Terminal Help  
[root@amilicevic ~]# pd auxZ | grep httpd  
-bash: pd: command not found  
[root@amilicevic ~]# ps auxZ | grep httpd  
unconfined_u:system_r:httpd_t:s0 root      5725  0.0  0.3 11788 3336 ?        S  
s  20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5728  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5729  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5730  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5731  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5732  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5733  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5734  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:system_r:httpd_t:s0 apache    5735  0.0  0.2 11788 2156 ?        S  
20:11  0:00 /usr/sbin/httpd  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 5787 0.0  0.0 4352 75  
2 pts/0 S+ 20:14  0:00 grep httpd  
[root@amilicevic ~]#
```

контекст безопасности. [root@amilicevic ~]#

Посмотрела текущее состояние переключателей SELinux для Apache с помощью ко-

```
root@amilicevic:~  
File Edit View Search Terminal Help  
user_ttyfile_stat off  
varnishd_connect_any off  
vbetool_mmap_zero_ignore off  
virt_use_comm off  
virt_use_execmem off  
virt_use_fusefs off  
virt_use_nfs off  
virt_use_samba off  
virt_use_sanlock off  
virt_use_sysfs on  
virt_use_usb on  
virt_use_xserver off  
webadm_manage_user_files off  
webadm_read_user_files off  
wine_mmap_zero_ignore off  
xdm_exec_bootloader off  
xdm_sysadm_login off  
xen_use_nfs off  
xguest_connect_network on  
xguest_mount_media on  
xguest_use_bluetooth on  
xserver_object_manager off  
zabbix_can_network off  
[root@amilicevic ~]#
```

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`

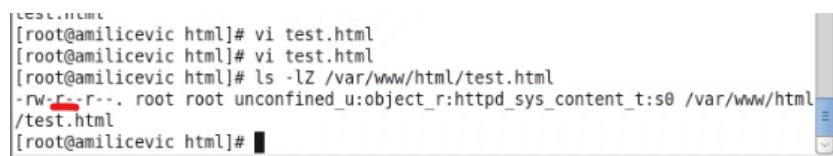
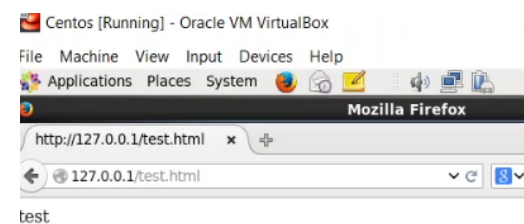


Рис. 0.6: Рис. 9.



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 -lZ /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 -lZ /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.

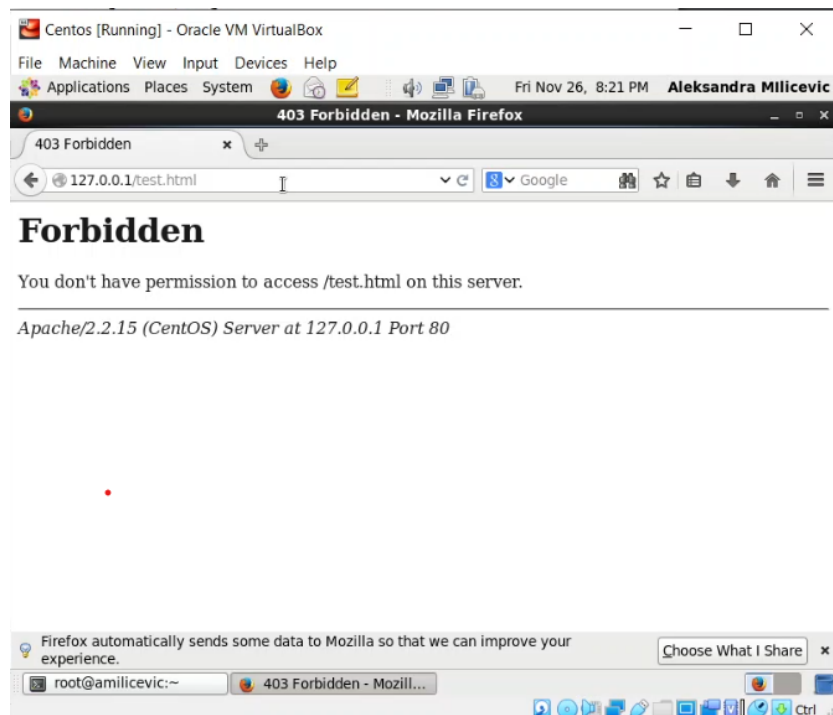


Рис. 0.9: Рис. 13.

```
[root@amilicevic ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Nov 26 20:19 /var/www/html/test.html
[root@amilicevic ~]#
```

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

```
[root@amilicevic ~]# tail /var/log/messages
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> gateway 10.0.2.2
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> nameserver '192.168.1.254'
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> domain name 't-com.me'
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit) scheduled...
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> Activation (eth0) Stage 4 of 5 (IP4 Configure Get) complete.
Nov 26 20:10:17 amilicevic NetworkManager[1342]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit) started...
Nov 26 20:10:18 amilicevic NetworkManager[1342]: <info> (eth0): device state change: ip-config -> activated (reason 'none') [7 8 0]
Nov 26 20:10:18 amilicevic NetworkManager[1342]: <info> Policy set 'System eth0' (eth0) as default for IPv4 routing and DNS.
Nov 26 20:10:18 amilicevic NetworkManager[1342]: <info> Activation (eth0) successful, device activated.
Nov 26 20:10:18 amilicevic NetworkManager[1342]: <info> Activation (eth0) Stage 5 of 5 (IP Configure Commit) complete.
[root@amilicevic ~]#
```

```

root@amilicevic ~]# tail -n1 /var/log/messages
lov 26 20:32:01 amilicevic rsyslogd: [origin software="rsyslogd" swVersion="5.8.
.0" x-pid="1268" x-info="http://www.rsyslog.com"] rsyslogd was HUPed

```

Рис. 0.11: Рис. 16.

в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81. Проанализировала 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)

```

[root@amilicevic ~]# cat /var/log/httpd/error_log
[Fri Nov 26 20:11:19 2021] [notice] SELinux policy enabled; httpd running as con
text unconfined u:system r:httpd t:s0
[Fri Nov 26 20:11:19 2021] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin
/suexec)
[Fri Nov 26 20:11:19 2021] [notice] Digest: generating secret for digest authent
ication ...
[Fri Nov 26 20:11:19 2021] [notice] Digest: done
[Fri Nov 26 20:11:19 2021] [warn] /mod_dnssd.c: No services found to register
[Fri Nov 26 20:11:19 2021] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- res
uming normal operations
[Fri Nov 26 20:20:11 2021] [error] [client 127.0.0.1] File does not exist: /var/
www/html/favicon.ico
[Fri Nov 26 20:20:11 2021] [error] [client 127.0.0.1] File does not exist: /var/
www/html/favicon.ico
[Fri Nov 26 20:21:58 2021] [error] [client 127.0.0.1] (13)Permission denied: acc
ess to /test.html denied
[root@amilicevic ~]#

```

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

```

acct="root" exe="/bin/su" noName="r" addr="r" terminal="pts/0" res="success"
[root@amilicevic ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@amilicevic ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'?

```

## Выводы

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