

## 0.1 Front matter

title: "Лабораторная работа №6" subtitle: "Основы информационной безопасности"  
author: "Пинега Белла Александровна"

## 0.2 Generic options

lang: ru-RU toc-title: "Содержание"

## 0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

## 0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables  
fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia  
polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true  
polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs:  
english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT  
Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions:  
Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9  
## Biblatex biblatex: true biblio-style: "gost-numeric" biblatexoptions: - parenttracker=true  
- backend=biber - hyperref=auto - language=auto - autolang=other\* - citestyle=gost-  
numeric ## Pandoc-crossref LaTeX customization figureTitle: "Рис." tableTitle: "Таблица"  
listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle: "Список таблиц" lolTitle:  
"Листинги" ## Misc options indent: true header-includes: -

## keep figures where there are in the text

– # keep figures where there are in the text

## 1 Цель работы

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

## 2 Задание

Загрузите в дисплейном классе операционную систему Linux. Осуществите вход в систему. Запустите терминал. Перейдите в каталог /var/tmp: `cd /var/tmp` Создайте каталог с именем пользователя (совпадающий с логином студента в дисплейном классе). Для этого можно использовать команду: `mkdir /var/tmp/id -un` или

непосредственно: `mkdir /var/tmp/имя_пользователя` Здесь вместо `имя_пользователя` должен быть указан ваш логин (учётная запись) в дисплейном классе. Запустите виртуальную машину, введя в командной строке:

Информационная безопасность компьютерных сетей 11 Рис. 1.6. Окно определения формата виртуального жёсткого диска Рис. 1.7. Окно определения размера виртуального динамического жёсткого диска и его расположения После завершения установки операционной системы корректно переза-пустите виртуальную машину (рис. 1.18) и при запросе примите условия лицензии (рис. 1.19–1.20). Рис. 1.8. Окно «Носители» виртуальной машины: подключение образа оптического диска Рис. 1.9. Запуск виртуальной машины В VirtualBox оптический диск должен отключиться автоматически, но если это не произошло, то необходимо отключить носитель информации с обра-зом, выбрав Свойства Носители Rocky-номер-версии.iso Удалить устройство . Информационная безопасность компьютерных сетей 13 Рис. 1.10.

Установка английского языка интерфейса ОС Войдите в ОС под заданной вами при установке учётной записью. В меню Устройства виртуальной машины подключите образ диска дополнений госте-вой ОС (рис. 1.21, 1.22), при необходимости введите пароль пользователя `root` вашей виртуальной ОС. После загрузки дополнений нажмите Return или Enter и корректно переза-грузите виртуальную машину. 14

Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.11. Окно настройки установки образа ОС Рис. 1.12. Окно настройки установки: выбор программ 1.3.1. Установка имени пользователя и названия хоста Если при установке виртуальной машины вы задали имя пользователя или имя хоста, не удовлетворяющее соглашению об именовании (см. раздел 1.2.2), то вам необходимо исправить это. 1. Запустите виртуальную машину и залогиньтесь. 2. Запустите терминал и получите полномочия администратора: `su` - Информационная безопасность компьютерных сетей 15 Рис. 1.13. Окно настройки установки: отключение KDUMP Рис. 1.14. Окно настройки установки: место установки 3. Создайте пользователя (вместо `username` укажите ваш логин в дисплей-ном классе): `adduser -G wheel username` 4. Задайте пароль для пользователя (вместо `username` укажите ваш логин в дисплейном классе): `passwd username` 16 Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.15. Окно настройки установки: сеть и имя узла Рис. 1.16. Установка пароля для `root` 5. Установите имя хоста (вместо `username` укажите ваш логин в дисплейном классе): `hostnamectl set-hostname username` 6. Проверьте, что имя хоста установлено верно: `hostnamectl` Информационная безопасность компьютерных сетей 17 Рис. 1.17.

Установка пароля для пользователя с правами администратора Рис. 1.18.

Завершение установки ОС 1.4. Домашнее задание Дождитесь загрузки графического окружения и откройте терминал. В окне терминала проанализируйте последовательность загрузки системы, выпол-нив команду `dmesg`. Можно просто просмотреть вывод этой команды: 18 Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.19. Первоначальная настройка ОС: переход к лицензии Рис. 1.20.

Первоначальная настройка ОС: лицензия `dmesg | less` Информационная безопасность компьютерных сетей 19 Рис. 1.21. Подключение образа диска дополнений гостевой ОС Рис. 1.22. Запуск образа диска дополнений гостевой ОС Можно использовать поиск с помощью `grep`: `dmesg | grep -i "то, что ищем"` Получите следующую информацию. 1. Версия ядра Linux (Linux version). 2. Частота процессора (Detected Mhz processor). 3. Модель процессора (CPU0). 4. Объем доступной оперативной

памяти (Memory available). 5. Тип обнаруженного гипервизора (Hypervisor detected). 6. Тип файловой системы корневого раздела. 20 Кулябов Д. С., Королькова А. В., Геворкян М. Н. 7. Последовательность монтирования файловых систем # Теоретическое введение

1.2.1. Техническое обеспечение Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (<https://www.virtualbox.org/>) операционной системы Linux (дистрибутив Rocky (<https://rockylinux.org/>)). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs.dk.sci.pfu.edu.ru/common/files/iso/). 1.2.2. Соглашения об именовании При выполнении работ следует придерживаться следующих правил именования: имя виртуальной машины, имя хоста вашей виртуальной машины, пользователь внутри виртуальной машины должны совпадать с логином студента, выполняющего лабораторную работу. Вы можете посмотреть ваш логин, набрав в терминале ОС типа Linux команду `id -un`.

### 3 Выполнение лабораторной работы

1. Проверю, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обращусь с помощью браузера к веб-серверу, запущенному на компьютере, он не работал - запустила.

```

[bapinega@bapinega ~]$ getenforce
Permissive
[bapinega@bapinega ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  permissive
Mode from config file:        enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
[bapinega@bapinega ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[bapinega@bapinega ~]$ 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: enabled)
   Active: active (running) since Wed 2024-02-21 19:47:18 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 11041 (httpd)
    Status: "Started, listening on: port 80"
[bapinega@bapinega ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[bapinega@bapinega ~]$ 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: enabled)
   Active: active (running) since Wed 2024-02-21 19:47:18 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 11041 (httpd)
    Status: "Started, listening on: port 80"
   Tasks: 213 (limit: 12167)
  Memory: 23.8M
   CGroup: /system.slice/httpd.service
           └─11041 /usr/sbin/httpd -DFOREGROUND
             └─11060 /usr/sbin/httpd -DFOREGROUND
               └─11061 /usr/sbin/httpd -DFOREGROUND
                 └─11063 /usr/sbin/httpd -DFOREGROUND
                   └─11064 /usr/sbin/httpd -DFOREGROUND

фев 21 19:47:13 bapinega.localdomain systemd[1]: Starting The Apache HTTP Server:
фев 21 19:47:18 bapinega.localdomain systemd[1]: Started The Apache HTTP Server:
фев 21 19:47:19 bapinega.localdomain httpd[11041]: Server configured, listening

```

## 2. Найдите веб-сервер Apache в списке процессов, его контекст безопасности

```

[bapinega@bapinega ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      11041  0.0  0.5 265108 11556 ?
Ss   19:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   11060  0.0  0.4 269812  8404 ?
S    19:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   11061  0.0  0.7 1458732 14236 ?
Sl   19:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   11063  0.0  0.6 1327604 12240 ?
Sl   19:47   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache   11064  0.0  0.5 1327604 10200 ?
Sl   19:47   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023 bapinega 11479 0.0  0.0 22
1940 1080 pts/1 S+  19:52   0:00 grep --color=auto httpd

```

3. Текущее состояние переключателей SELinux для Apache

```
[bapinega@bapinega ~]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_redis off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
```

4. Тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html

```
[bapinega@bapinega ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 апр 18 2
023 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр 18 2
023 html
[bapinega@bapinega ~]$ su
Пароль:
[root@bapinega bapinega]# cd /var/www/html
[root@bapinega html]# touch test.html
[root@bapinega html]# ls
test.html
```

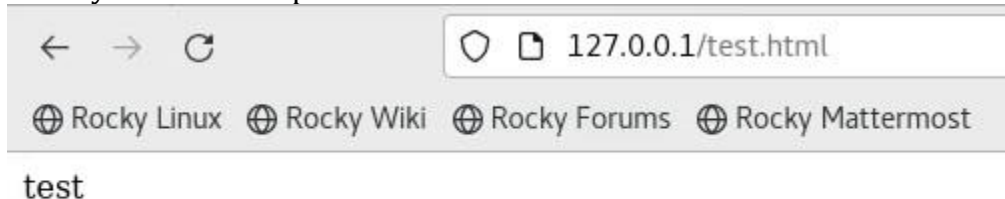
Создам от имени суперпользователя html-файл /var/www/html/test.html

```
[root@bapinega html]# cat test.html
<html>
<body>test</body>
```

следующего содержания:

Успешно

5. Файл успешно отображен





6. Для httpd определен контекст файла httpd\_sys\_content\_t

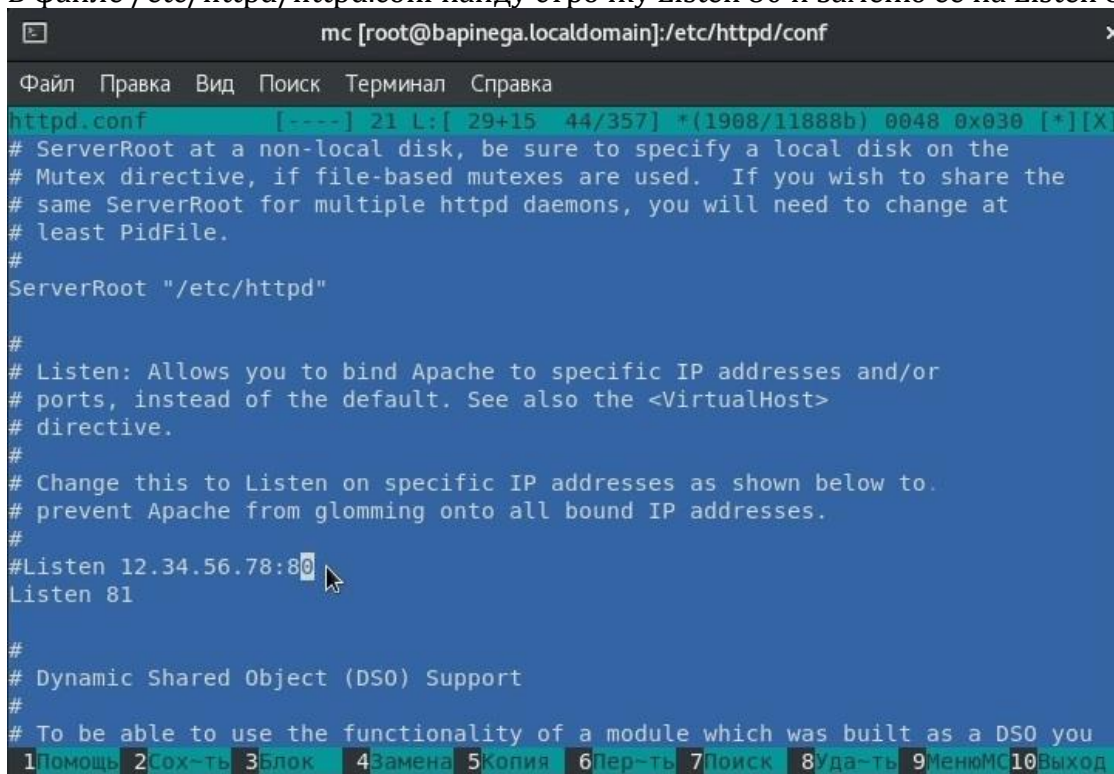
```
[bapinega@bapinega httpd]$ man httpd
[bapinega@bapinega httpd]$ ls -z test.html
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[bapinega@bapinega httpd]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[bapinega@bapinega httpd]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Операция не позволена
[bapinega@bapinega httpd]$ su
Пароль:
[root@bapinega httpd]# chcon -t samba_share_t /var/www/html/test.html
[root@bapinega httpd]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Изменяю контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t: Успешно

7. Файл не был отображён, тк запущены процессы setroubleshootd и audtd.  
Смотрю системный лог-файл:

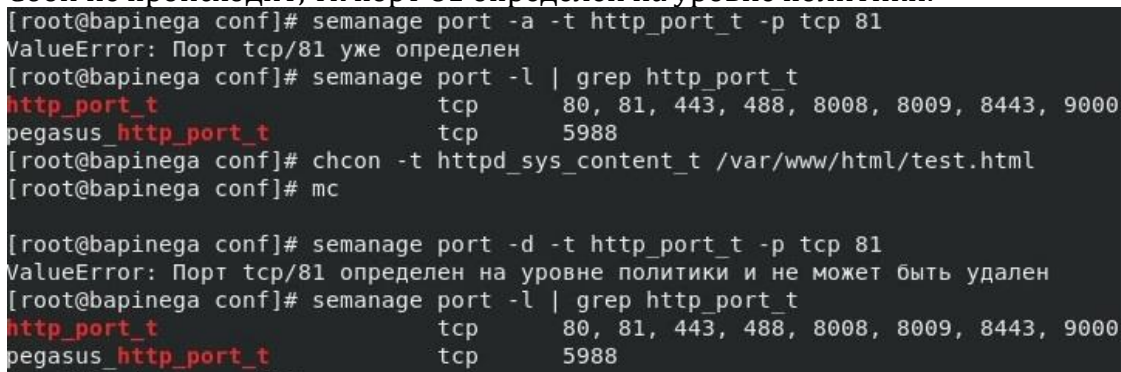
```
[root@bapinega httpd]# tail /var/log/messages
system is too slow
Feb 21 20:25:42 bapinega org.gnome.Shell.desktop[1989]: libinput error: client bug: timer event4 debounce: scheduled expiry is in the past (-263ms), your system is too slow
Feb 21 20:25:42 bapinega org.gnome.Shell.desktop[1989]: libinput error: client bug: timer event4 debounce short: scheduled expiry is in the past (-276ms), your system is too slow
Feb 21 20:26:33 bapinega org.gnome.Shell.desktop[1989]: libinput error: client bug: timer event4 debounce: scheduled expiry is in the past (-196ms), your system is too slow
Feb 21 20:26:33 bapinega org.gnome.Shell.desktop[1989]: libinput error: client bug: timer event4 debounce short: scheduled expiry is in the past (-209ms), your system is too slow
Feb 21 20:28:20 bapinega dbus-daemon[781]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.783' (uid=0 pid=13532 comm="su " label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023")
Feb 21 20:28:20 bapinega systemd[1]: Starting Fingerprint Authentication Daemon.
..
Feb 21 20:28:20 bapinega dbus-daemon[781]: [system] Successfully activated service 'net.reactivated.Fprint'
Feb 21 20:28:20 bapinega systemd[1]: Started Fingerprint Authentication Daemon.
Feb 21 20:28:22 bapinega su[13532]: (to root) bapinega on pts/1
```

8. В файле `/etc/httpd/httpd.conf` найду строчку `Listen 80` и заменю её на `Listen 81`



```
mc [root@bapinega.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf [----] 21 L:[ 29+15 44/357] *(1908/11888b) 0048 0x030 [*][X]
# 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 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
1Помощь 2Сох-ть 3Блок 4Замена 5Копия 6Пер-ть 7Поиск 8Уда-ть 9МенюМС 10Выход
```

9. Сбой не происходит, тк порт 81 определен на уровне политики.



```
[root@bapinega conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@bapinega conf]# 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@bapinega conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@bapinega conf]# mc

[root@bapinega conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@bapinega conf]# 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
```

{#fig:012width=70%} Исправьте обратно конфигурационный файл apache, вернув `Listen 80`. Удалю привязку `http_port_t` к 81 порту

10. Удалю файл `/var/www/html/test.html`:



```
[root@bapinega conf]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
```

## 4 Выводы

Мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache

## Список литературы