

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №9

дисциплина: Основы администрирования операционных систем

Студент: _

Группа: ____

МОСКВА

2024 г.

Постановка задачи

Получить навыки работы с контекстом безопасности и политиками SELinux.

Выполнение работы

Управление режимами SELinux

1. Запустите терминал и получите полномочия администратора: `su -`
2. Просмотрите текущую информацию о состоянии SELinux: `sestatus -v` В отчёте построчно поясните выведенную на экран информацию.
3. Посмотрите, в каком режиме работает SELinux: `getenforce` По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing).
4. Измените режим работы SELinux на разрешающий (Permissive): `setenforce 0` и снова введите `getenforce`

```
root@localhost: ~  
[zashikhalievaa@localhost ~]$ sudo -i  
[sudo] пароль для zashikhalievaa:  
[root@localhost ~]# sestatus -v  
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  
  
Process contexts:  
Current context:             unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
Init context:               system_u:system_r:init_t:s0  
/usr/sbin/sshd              system_u:system_r:sshd_t:s0-s0:c0.c1023  
  
File contexts:  
Controlling terminal:       unconfined_u:object_r:user_devpts_t:s0  
/etc/passwd                 system_u:object_r:passwd_file_t:s0  
/etc/shadow                 system_u:object_r:shadow_t:s0  
/bin/bash                   system_u:object_r:shell_exec_t:s0  
/bin/login                  system_u:object_r:login_exec_t:s0  
/bin/sh                     system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0  
/sbin/agetty                system_u:object_r:getty_exec_t:s0  
/sbin/init                  system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0  
/usr/sbin/sshd              system_u:object_r:sshd_exec_t:s0  
[root@localhost ~]#
```

5. В файле `/etc/sysconfig/selinux` с помощью редактора установите `SELINUX=disabled`
Перезагрузите систему.

```
root@localhost:~
selinux [-----] 0 L:[ 1+ 0 1/ 30] *(0 /1263b) 0010 0x00A [*][X]

This file controls the state of SELinux on the system.
SELINUX= can take one of these three values:
    enforcing - SELinux security policy is enforced.
    permissive - SELinux prints warnings instead of enforcing.
    disabled - No SELinux policy is loaded.
See also:
https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/9/html/

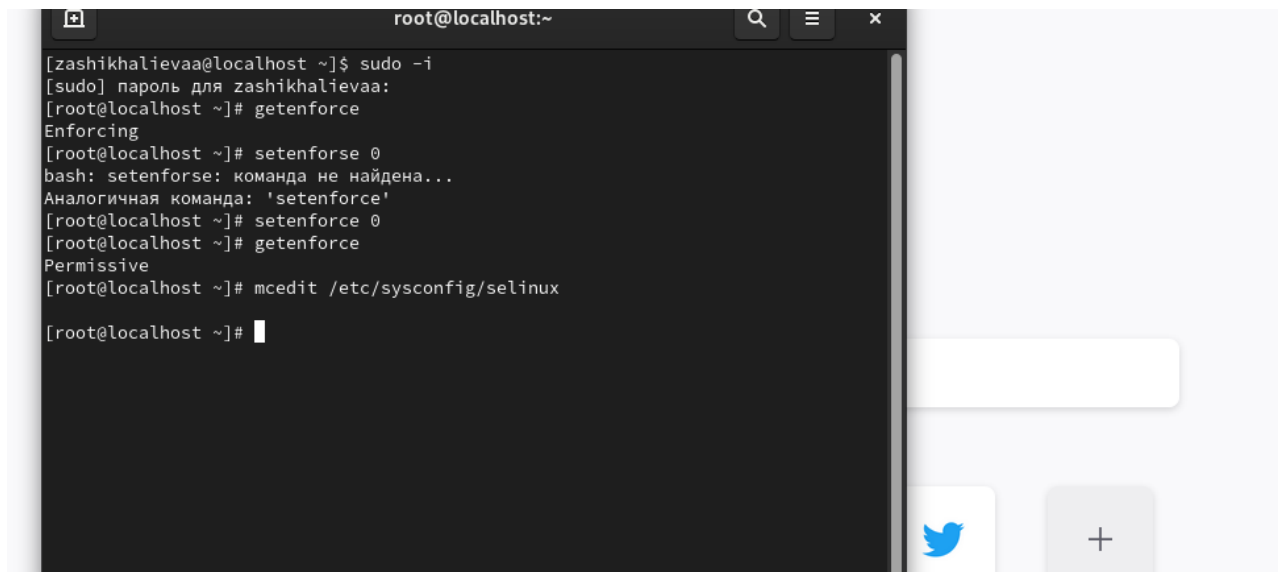
NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
fully disable SELinux during boot. If you need a system with SELinux
fully disabled instead of SELinux running with no policy loaded, you
need to pass selinux=0 to the kernel command line. You can use grubby
to persistently set the bootloader to boot with selinux=0:

    grubby --update-kernel ALL --args selinux=0

To revert back to SELinux enabled:

    grubby --update-kernel ALL --remove-args selinux

SELINUX=enforcing
1Помощь 2Сох~ть 3Блок 4Замена 5Копия 6Пер~ть 7Поиск 8Уда~ть 9МенюМС10Выход
```

A terminal window titled 'root@localhost:~' with search, menu, and close icons. The terminal shows a user 'zashikhalievaa' running 'sudo -i' and entering a password. As root, they run 'getenforce' (returns 'Enforcing'), 'setenforce 0' (returns an error), and 'setenforce 0' again (returns 'Permissive'). Finally, they run 'mcedit /etc/sysconfig/selinux'.

```
root@localhost:~  
[zashikhalievaa@localhost ~]$ sudo -i  
[sudo] пароль для zashikhalievaa:  
[root@localhost ~]# getenforce  
Enforcing  
[root@localhost ~]# setenforce 0  
bash: setenforce: команда не найдена...  
Аналогичная команда: 'setenforce'  
[root@localhost ~]# setenforce 0  
[root@localhost ~]# getenforce  
Permissive  
[root@localhost ~]# mcedit /etc/sysconfig/selinux  
[root@localhost ~]#
```

6. После перезагрузки запустите терминал и получите полномочия администратора.
7. Посмотрите статус SELinux: `getenforce` Вы увидите, что SELinux теперь отключён.
8. Попробуйте переключить режим работы SELinux: `setenforce 1` Какая реакция системы? Вы не можете переключаться между отключённым и принудительным режимом без перезагрузки системы.

9. Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите: `SELINUX=enforcing` Перезагрузите систему.

```
selinux [----] 0 L:[ 1+ 0 1/ 30] *(0 /1263b) 0010 0x00A [*][X]
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
```

10. Во время загрузки системы вы, скорее, всего получите предупреждающее сообщение о необходимости восстановления меток SELinux, что может занять некоторое время, а также потребует дополнительной перезагрузки системы.

```
Booting `Rocky Linux (5.14.0-427.13.1.el9_4.x86_64) 9.4 (Blue Unix)`
[ 2.714651] systemd[1]: Invalid DMI field header.
[ 4.173885] Warning: Unmaintained driver is detected: e1000
[ 4.774817] vmgfx 0000:00:02.0: [drm] *ERROR* vmgfx seems to be running on
an unsupported hypervisor.
[ 4.774820] vmgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 4.774823] vmgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 17.571236] selinux-autorelabel[726]: *** Warning -- SELinux targeted policy relabel is required.
[ 17.571597] selinux-autorelabel[726]: *** Relabeling could take a very long time, depending on file
[ 17.571930] selinux-autorelabel[726]: *** system size and speed of hard drives.
[ 17.654151] selinux-autorelabel[726]: Running: /sbin/fixfiles -T 0 restore
[ 38.538496] selinux-autorelabel[732]: Warning: Skipping the following R/O filesystems:
[ 38.531861] selinux-autorelabel[732]: /run/credentials/systemd-sysctl.service
[ 38.532988] selinux-autorelabel[732]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 38.533653] selinux-autorelabel[732]: /run/credentials/systemd-tmpfiles-setup.service
[ 38.534364] selinux-autorelabel[732]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/kerne
l/debug /sys/kernel/tracing
```

11. После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux: `sestatus -v` Убедитесь, что система работает в принудительном режиме (enforcing) SELinux.

```
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

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                        system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                   system_u:object_r:getty_exec_t:s0
/sbin/init                     system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

Использование restorecon для восстановления контекста безопасности

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите контекст безопасности файла /etc/hosts: `ls -Z /etc/hosts` Вы увидите, что у файла есть метка контекста `net_conf_t`.
3. Скопируйте файл /etc/hosts в домашний каталог: `cp /etc/hosts ~/` Проверьте контекст файла ~/hosts: `ls -Z ~/hosts` Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет `admin_home_t`.
4. Попробуйте перезаписать существующий файл hosts из домашнего каталога в каталог /etc: `mv ~/hosts /etc` и подтвердите, что вы хотите сделать это.
5. Убедитесь, что тип контекста по-прежнему установлен на `admin_home_t`: `ls -Z /etc/hosts`
6. Исправьте контекст безопасности: `restorecon -v /etc/hosts` Опция `-v` покажет процесс изменения.
7. Убедитесь, что тип контекста изменился: `ls -Z /etc/hosts`
8. Для массового исправления контекста безопасности на файловой системе введите `touch /.autorelabel` и перезагрузите систему. Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения. Вы увидите, что файловая система автоматически перемаркирована.

```
[root@localhost ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@localhost ~]# cp /etc/hosts ~
[root@localhost ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@localhost ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@localhost ~]# mv ~/hosts /etc/
mv: переписать '/etc/hosts'? y
[root@localhost ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@localhost ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:
object_r:net_conf_t:s0
[root@localhost ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@localhost ~]#
```

```
Файл  Массив  Bus  Блок  Устройство  Состояние
2.051651] systemd[1]: Invalid DMI field header.
4.399685] Warning: Unmaintained driver is detected: e1000
4.040352] vmwgfx: 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
4.040355] vmwgfx: 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
4.040357] vmwgfx: 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
12.944302] selinux-autorelabel[7251]: *** Warning -- SELinux targeted policy relabel is required.
12.944855] selinux-autorelabel[7251]: *** Relabeling could take a very long time, depending on file
12.945154] selinux-autorelabel[7251]: *** system size and speed of hard drives.
10.009604] selinux-autorelabel[7251]: Running: /sbin/fixfiles -T 0 restore
32.960215] selinux-autorelabel[7311]: Warning: Skipping the following R/O filesystems:
32.961257] selinux-autorelabel[7311]: /run/credentials/systemd-sysctl.service
32.961919] selinux-autorelabel[7311]: /run/credentials/systemd-tmpfiles-setup-dev.service
32.962404] selinux-autorelabel[7311]: /run/credentials/systemd-tmpfiles-setup.service
32.963212] selinux-autorelabel[7311]: Relabeling / /boot /dev /dev/hugepages /dev/queue /dev/pts /dev/shm /run /sys /sys/fs/cgroup /sys/fs/pstore /sys/ker
n/debug /sys/kernel/tracing
```

Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запустите терминал и получите полномочия администратора.
2. Установите необходимое программное обеспечение: `dnf -y install httpd dnf -y install lynx`
3. Создайте новое хранилище для файлов веб-сервера: `mkdir /web`
4. Создайте файл `index.html` в каталоге с контентом веб-сервера: `cd /web touch index.html` и поместите в файл следующий текст: `Welcome to my web-server`

```
Rocky Linux 9 - BaseOS                               135 kB/s | 2.3 MB   00:17
Rocky Linux 9 - AppStream                             4.8 kB/s | 4.5 kB   00:00
Rocky Linux 9 - AppStream                             4.0 MB/s | 8.0 MB   00:01
Rocky Linux 9 - Extras                               2.9 kB/s | 2.9 kB   00:01
Rocky Linux 9 - Extras                               11 kB/s | 15 kB    00:01
Package httpd-2.4.57-11.el9_4.1.x86_64 is already installed.
Dependencies resolved.
=====
Package           Architecture      Version           Repository         Size
=====
Installing:
lynx               x86_64            2.8.9-20.el9      appstream           1.5 M
Transaction Summary
=====
• Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm                          2.3 MB/s | 1.5 MB   00:00
-----
Total                                                  1.4 MB/s | 1.5 MB   00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : lynx-2.8.9-20.el9.x86_64       1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64     1/1
  Verifying      : lynx-2.8.9-20.el9.x86_64       1/1

Installed:
lynx-2.8.9-20.el9.x86_64
```


5. В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot "/var/www/html" и ниже добавьте строку DocumentRoot "/web". Затем в этом же файле ниже закомментируйте раздел AllowOverride None Require all granted и добавьте следующий раздел, определяющий правила доступа: AllowOverride None Require all granted

```
httpd.conf [-----] 1 L:[110+22 132/367] *(4618/12135b) 0047 0x02F [*]
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#DocumentRoot "/var/www/html"
DocumentRoot "/web"

<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>

#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#     AllowOverride None
#     # Allow open access:
#     Require all granted
#</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

6. Запустите веб-сервер и службу http: `systemctl start httpd` `systemctl enable httpd`

7. В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: `lynx http://localhost` вы увидите веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла `index.html`. В нижней части терминала с lynx указаны подсказки по навигации. Для выхода из lynx нажмите `q`.

```
HTTP Server Test Page

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky Linux system. If you can read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or could be going through maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you've expected, you should send them an email. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproduceable platform based on the sources of Red Hat Enterprise Linux (RHEL). With this in mind, please understand that:
* Neither the Rocky Linux Project nor the Rocky Enterprise Software Foundation have anything to do with this website or its content.
* The Rocky Linux Project nor the RESF have "hacked" this webserver: This test page is included with the distribution.

For more information about Rocky Linux, please visit the Rocky Linux website.

I am the admin, what do I do?

You may now add content to the webroot directory for your software.


For systems using the Apache Webserver: You can add content to the directory /var/www/html/. Until you do so, people visiting your website will see this page. If you would like this page to not be shown, follow the instructions in: /etc/httpd/conf.d/welcome.conf.

For systems using Nginx: You can add your content in a location of your choice and edit the root
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
```

8. В терминале с полномочиями администратора примените новую метку контекста к /web:
`semanage fcontext -a -t httpd_sys_content_t "/web(/.*)"?"`

9. Восстановите контекст безопасности: `restorecon -R -v /web`

10. В терминале под учётной записью своего пользователя снова обратитесь к веб-серверу:
`lynx http://localhost` Теперь вы получите доступ к своей пользовательской веб-странице. Если этого не произошло, то перезагрузите систему и снова попытайтесь получить доступ к своей пользовательской веб-странице. В случае успеха на экране должна быть отображена запись «Welcome to my web-server».



```
Welcome to my web-server
```

Работа с переключателями SELinux

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите список переключателей SELinux для службы ftp: `getsebool -a | grep ftp` Вы увидите переключатель `ftpd_anon_write` с текущим значением `off`.
3. Для службы `ftpd_anon` посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: `semanage boolean -l | grep ftpd_anon`
4. Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`:
`setsebool ftpd_anon_write on`
5. Повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`:
`getsebool ftpd_anon_write`
6. Посмотрите список переключателей с пояснением: `semanage boolean -l | grep ftpd_anon`
Обратите внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.
7. Измените постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`:
`setsebool -P ftpd_anon_write on`
8. Посмотрите список переключателей: `semanage boolean -l | grep ftpd_anon` В отчёте отразите, какое состояние имеет переключатель?

Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

Чтобы временно переключить SELinux в разрешающий (permissive) режим, используйте команду: `setenforce 0`

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

Для отображения всех переключателей (булевых переменных) SELinux используйте команду: `getsebool -a`

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

Для удобного просмотра сообщений SELinux нужно установить пакет: `setroubleshoot`

4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?

Примените контекст следующими командами:

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

```
restorecon -Rv /web
```

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

Чтобы полностью отключить SELinux, измените файл конфигурации: `/etc/selinux/config`

Для полного отключения SELinux измените файл конфигурации: `/etc/selinux/config`

Найдите строку: `SELINUX=enforcing`

И замените её на: `SELINUX=disabled`

6. Где SELinux регистрирует все свои сообщения?

Сообщения SELinux регистрируются в следующих файлах:

`/var/log/audit/audit.log` — для аудита,

`/var/log/messages` — для общих сообщений.

7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию?

Чтобы узнать доступные типы контекста для службы FTP, используйте команду: `seinfo -t`

Или для конкретного поиска: `sesearch --allow -s ftpd_t -t`

8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

Самый простой способ — временно переключить SELinux в режим `permissive`:

`setenforce 0`

Затем проверьте работу сервиса. Если проблема исчезла, значит, она связана с SELinux.

Заключение

Получены навыки работы с SELinux.