

Отчёта по лабораторной работе №9

Отчет

Зубов Иван Александрович

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Управление режимами SELinux	6
3.2	Использование restorecon для восстановления контекста безопасности	8
3.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	8
3.4	Работа с переключателями SELinux	11
4	Выводы	12
5	Контрольные вопросы	13

Список иллюстраций

3.1	Смотрим информацию	7
3.2	Изменяем режим	7
3.3	Редактируем файл	7
3.4	Проверяем контексты файлов	8
3.5	Изменяем тип контекста	8
3.6	Установка ПО	9
3.7	Создаем каталог и файл	9
3.8	Редактируем файл	10
3.9	Запускаем службу	10
3.10	Применяем новую метку контекста и восстановим метку безопасности	11
3.11	Welcome to my web-server	11
3.12	Работа с переключателями	11

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux
3. Настройте контекст безопасности для нестандартного расположения файлов вебслужбы
4. Продемонстрируйте навыки работы с переключателями SELinux

3 Выполнение лабораторной работы

3.1 Управление режимами SELinux

Получаем полномочия администратора и смотрим текущую информацию о состоянии SELinux

Построчное пояснение информации на экране

SELinux status: enabled — SELinux включен в системе. SELinuxfs mount — точка монтирования виртуальной ФС SELinux. SELinux root directory — корневая директория конфигурации SELinux. Loaded policy name: targeted — загружена политика «targeted» (ограничивает только определённые сервисы). Current mode: enforcing — текущий режим: принудительный (правила применяются). Mode from config file: enforcing — режим из конфигурационного файла тоже «enforcing». Policy MLS status: enabled — поддержка Multi-Level Security включена. Policy deny_unknown status: allowed — неизвестные действия по умолчанию разрешены. Memory protection checking — проверка защиты памяти активна. Max kernel policy version — максимальная версия политики, поддерживаемая ядром.

```
[root@iazubov ~]# 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
```

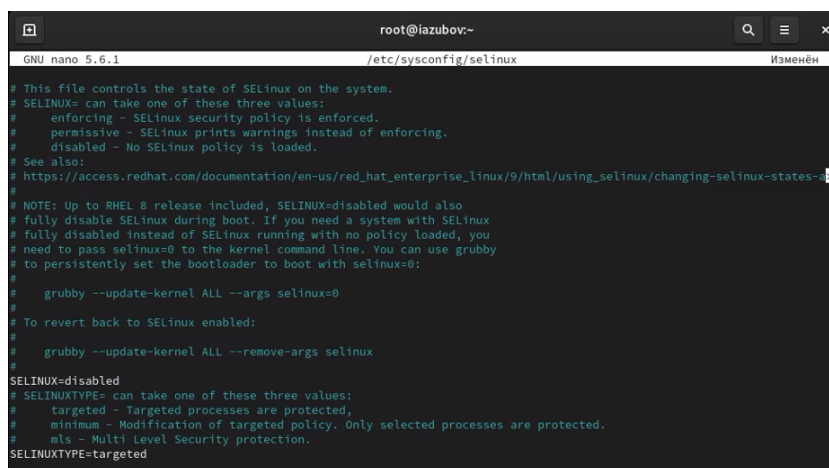
Рис. 3.1: Смотрим информацию

Посмотрим, в каком режиме работает SELinux и изменим режим работы SELinux на разрешающий (Permissive)

```
[root@iazubov ~]# getenforce
Enforcing
[root@iazubov ~]# setenforce 0
[root@iazubov ~]# getenforce
Permissive
[root@iazubov ~]# nano /etc/sysconfig/selinux
```

Рис. 3.2: Изменяем режим

Редактируем файл /etc/sysconfig/selinux и перезагружаем систему

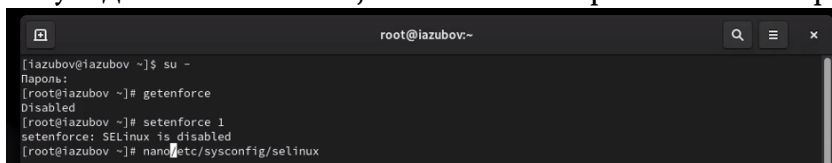


```
GNU nano 5.6.1 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELinux= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
#   https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing_selinux_states-1
#
# 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=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected.
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 3.3: Редактируем файл

Посмотрим статус SELinux и увидим, что он отключен. Переключаем режим работы. Далее откроем файл /etc/sysconfig/selinux с помо-

щью редактора и установим: SELINUX=enforcing. Перезагружаем систему. Во время перезагрузки мы получили предупреждающее сообщение и убедились потом, что система работает в принудительном режиме.



```
root@iazubov:~  
[iazubov@iazubov ~]$ su -  
Пароль:  
[root@iazubov ~]# getenforce  
Disabled  
[root@iazubov ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@iazubov ~]# nano /etc/sysconfig/selinux
```

3.2 Использование restorecon для восстановления контекста безопасности

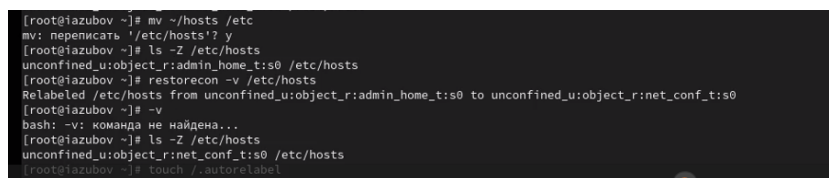
Посмотрите контекст безопасности файла /etc/hosts. Скопируйте файл /etc/hosts в домашний каталог и проверим контекст файла ~/hosts.



```
[root@iazubov ~]# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
[root@iazubov ~]# cp /etc/hosts ~/.  
[root@iazubov ~]# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
[root@iazubov ~]#
```

Рис. 3.4: Проверяем контексты файлов

Попытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc и изменим тип контекста.



```
[root@iazubov ~]# mv ~/hosts /etc  
mv: переписать '/etc/hosts'? y  
[root@iazubov ~]# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
[root@iazubov ~]# 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@iazubov ~]# -v  
bash: -v: команда не найдена...  
[root@iazubov ~]# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
[root@iazubov ~]# touch /.autorelabel
```

Рис. 3.5: Изменяем тип контекста

3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Устанавливаем программное обеспечение


```
root@iazubov-
[root@iazubov ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64          33 kB/s | 32 kB  00:00
Extra Packages for Enterprise Linux 9 - x86_64          5.7 MB/s | 20 MB 00:03
Extra Packages for Enterprise Linux 9 - x86_64          4.3 kB/s | 993 B 00:00
Rocky Linux 9 - BaseOS                                  11 kB/s | 4.1 kB 00:00
Rocky Linux 9 - BaseOS                                  3.1 MB/s | 2.5 MB 00:00
Rocky Linux 9 - AppStream                               12 kB/s | 4.5 kB 00:00
Rocky Linux 9 - AppStream                               4.8 MB/s | 9.5 MB 00:01
Rocky Linux 9 - Extras                                  7.3 kB/s | 2.9 kB 00:00
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@iazubov ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:23 назад, Ср 22 окт 2025 17:27:20.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Раз
=====
Установка:
lynx       x86_64       2.8.9-20.el9      appstream    1.5
=====
Результат транзакции
=====
Установка 1 Пакет

Объем загрузки: 1.5 М
Объем изменений: 6.1 М
Загрузка пакетов:
lynx-2.8.9-20.el9.x86_64.rpm          4.5 MB/s | 1.5 MB  00:00
-----
Общий размер
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка      :
Установка       : lynx-2.8.9-20.el9.x86_64
Запуск скрипта  : lynx-2.8.9-20.el9.x86_64
Проверка        : lynx-2.8.9-20.el9.x86_64
Установлен:
lynx-2.8.9-20.el9.x86_64
```

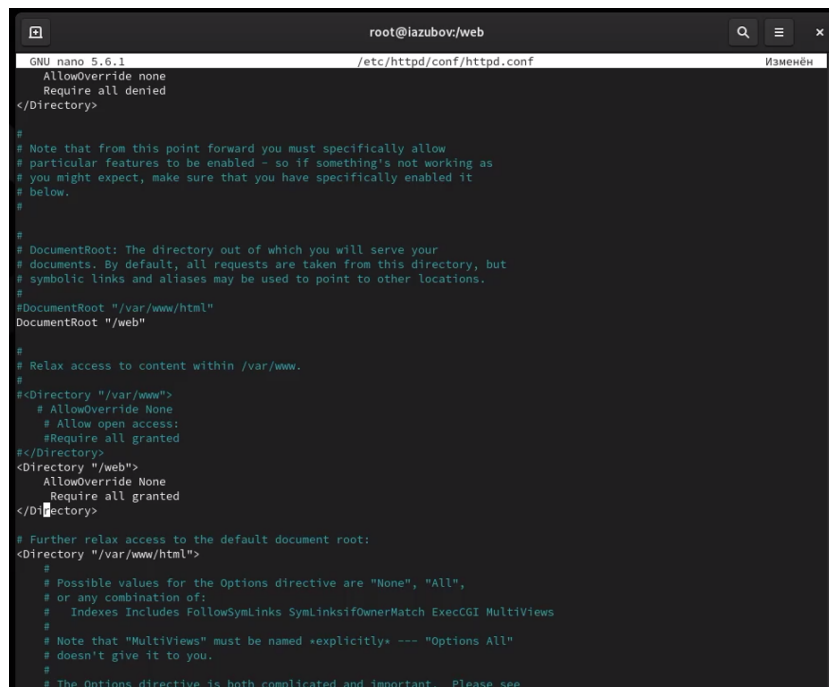
Рис. 3.6: Установка ПО

Создаем новое хранилище для файлов web-сервера и файл

```
[root@iazubov ~]# mkdir /web
[root@iazubov ~]# cd /web
[root@iazubov web]# touch index.html
[root@iazubov web]# nano index.html
```

Рис. 3.7: Создаем каталог и файл

С помощью редактора nano редактируем файл index.html



```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# AllowOverride none
# Require all denied
</Directory>

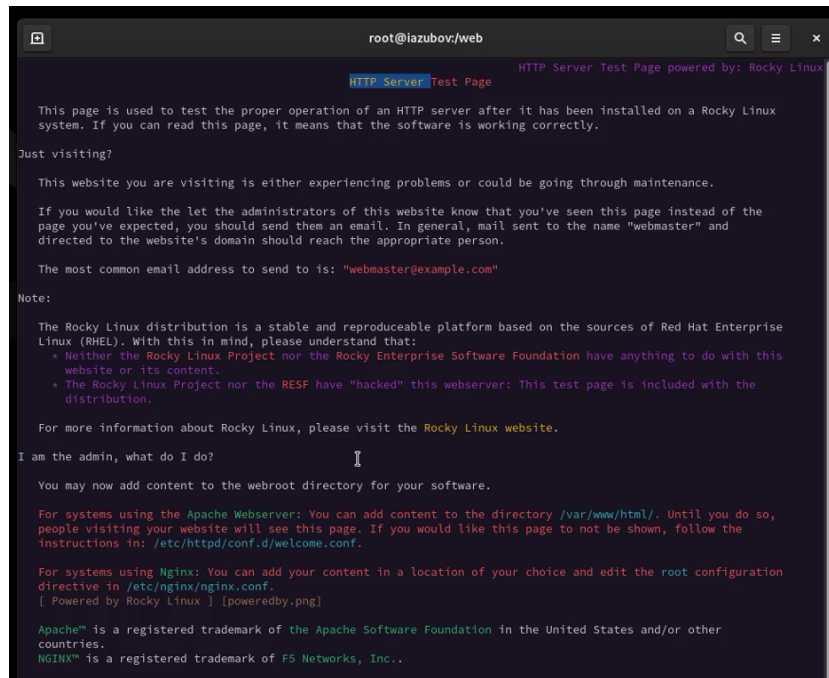
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, 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"

#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#   AllowOverride None
#   Allow open access:
#   Require all granted
#</Directory>
<Directory "/web">
    AllowOverride None
    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",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
```

Рис. 3.8: Редактируем файл

Запускаем веб сервер и службу httpd Запускаем веб страница. Она будет просто по умолчанию



```
HTTP Server Test Page HTTP Server Test Page powered by: Rocky Linux

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 the 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 configuration
directive in /etc/nginx/nginx.conf.
[ Powered by Rocky Linux ] [poweredby.png]

Apache® is a registered trademark of the Apache Software Foundation in the United States and/or other
countries.
NGINX® is a registered trademark of F5 Networks, Inc..
```

Рис. 3.9: Запускаем службу

В терминале применим новую метку контекста к /web и восстановим контекст безопасности

```
[root@iazubov web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@iazubov web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
[root@iazubov web]#
```

Рис. 3.10: Применяем новую метку контекста и восстановим метку безопасности

Запускаем наш веб сервер

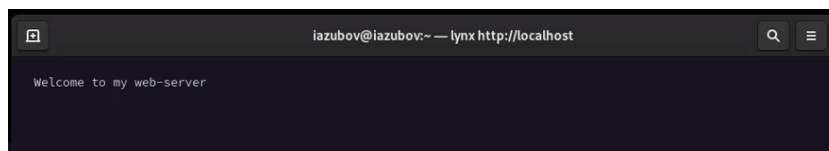


Рис. 3.11: Welcome to my web-server

3.4 Работа с переключателями SELinux

Смотрим списки переключателей и изменяем их

```
root@iazubov:~
[iazubov@iazubov ~]$ lynx http://localhost
[iazubov@iazubov ~]$ su -
iazubov:
[root@iazubov ~]# getsebool -a | grep ftp
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@iazubov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@iazubov ~]# setsebool ftpd_anon_write on
[root@iazubov ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@iazubov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write
[root@iazubov ~]# setsebool -P ftpd_anon_write on
[root@iazubov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл., вкл.) Allow ftpd to anon write
[root@iazubov ~]#
```

Рис. 3.12: Работа с переключателями

4 Выводы

Я получил навыки работы с контекстом безопасности и политиками SELinux.

5 Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? `setenforce 0`
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? `getsebool -a`
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? `selinux-policy-doc`
4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`? `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` `restorecon -R /web`
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? `/etc/selinux/config` (изменить `SELINUX=disabled`)
6. Где SELinux регистрирует все свои сообщения? `/var/log/messages`
7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию? `seinfo -t | grep ftp`
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? Временно перевести SELinux в режим `setenforce Permissive` и проверить работу сервиса