

Отчет о лабораторной работе

Лабораторная работа №9

Казначеев Сергей Ильич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Контрольные вопросы	16
4	Вывод	18

Список иллюстраций

2.1	1	6
2.2	2	7
2.3	3	8
2.4	4	8
2.5	5	8
2.6	6	8
2.7	7	9
2.8	8	9
2.9	9	9
2.10	10	10
2.11	11	10
2.12	12	10
2.13	13	11
2.14	14	11
2.15	15	11
2.16	16	11
2.17	17	12
2.18	18	12
2.19	19	12
2.20	20	12
2.21	21	13
2.22	22	13
2.23	23	13
2.24	24	14
2.25	25	14
2.26	26	14
2.27	27	15
2.28	28	15
2.29	29	15

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Для начала откроем терминал и перейдем в супер пользователя рис. 2.1).

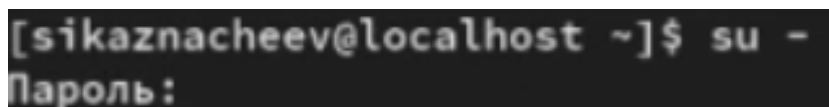


Рис. 2.1: 1

Далее посмотрим текущую информацию о состоянии SELinux на экран была выведена подробная сводка о состоянии и конфигурации SELinux

Строка 1 - пользователь то есть я на хосте localhost выполнил команду sestatus -v с правами суперпользователя Строка 2 - запрос пароля sudo система запросила пароль пользователя для предоставления прав суперпользователя Строка 3 - Общий статус SELinux был активирован в системе и функционирует Строка 4 - Виртуальная файловая система SELinux смонтирована в директории через эту файловую систему ядро предоставляет информацию о SELinux Строка 5 = основные конфигурационные файлы и политики SELinux расположены в директории /etc/selinux Строка 6 - Загружена политика безопасности типа targeted - защищаются только определенные системные службы остальные процессы работают без ограничений Строка 7 - SELinux работает в режиме принудительного применения политики - все нарушения блокируются Строка 8 - Режим enforcing установлен в конфигурационном файле и будет сохраняться после перезагрузки Строка 9 - поддержка Multi-level Security включена в политику Строка 10 - Политика разрешает доступ к объектам с неизвестными классами или разрешениями Строка 11 = SELinux проверяет защиту памяти на основе фактических безопасно-

сти Строка 12 - Ядро поддерживает политики SELinux до версии 33 включительно
 Строка 14 - начало раздела с контекстами безопасности текущих процессов Строка 15 - Текущая сессия пользователя работает в неограниченном домене сам домен Строка 16 - Основной системный процесс init работает в домене init_t Строка 17 - Домен ssh работает в ограниченном домене sshd_t с дополнительными уровнями безопасности Строка 19 - начало раздела с контекстами безопасности системных файлов Строка 20 - Управляющий терминал имеет тип user_devpts_t для псевдо терминалов Строка 21 - Файл с учетными записями пользователей имеет тип passwd_file_t Строка 22 - файл с хешами паролей имеет защищенный тип shadow_t Строка 23 - Исполняемый файл bash имеет тип shell_exec_t Строка 24 - Исполняемый файл login bvttn nbg login_exec_t Строка 25 - Символическая ссылка /bin/sh указывает на файл с типом shell_exec_t Строка 26 - Исполняемый файл agetty имеет тип getty_exec_t Строка 27 - исполняемый файл init имеет тип init_exec_t Строка 28 - Исполняемый файл ssh домена имеет тип ssh_exec_t

```

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

```

Рис. 2.2: 2

После чего посмотрим в каком режиме работает SELinux, затем изменим режим работы SELinux на разрешающий (Permissive)

```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
```

Рис. 2.3: 3

Далее запишем в файл /etc/sysconfig/selinux следующее SELINUX=disabled

```
# 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.
```

Рис. 2.4: 4

Перезагрузим систему

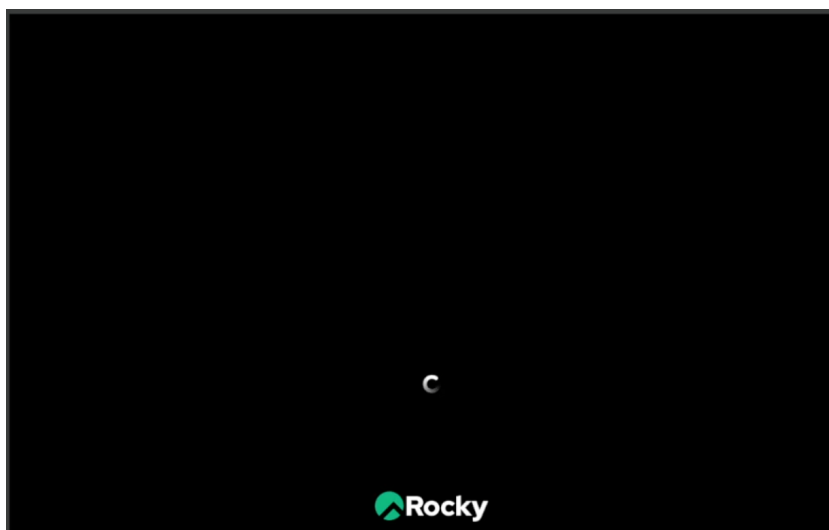


Рис. 2.5: 5

После перезагрузки посмотрим статус SELinux

```
[sikaznacheev@localhost ~]$ getenforce
Disable
```

Рис. 2.6: 6

Затем пробуем переключить режим работы SELinux

```
[sikaznacheev@localhost ~]$ setenforce 1  
setenforce: SELinux is disabled
```

Рис. 2.7: 7

После чего откроем файл /etc/sysconfig/selinux и изменим на SELINUX=enforcing

```
SELINUX=enforcing  
# SELINUXTYPE= can take one of these three values:  
#   targeted - Targeted processes are protected,  
#   minimum - Modification of targeted policy. Only selected processes  
#   mls - Multi Level Security protection.  
SELINUXTYPE=targeted
```

Рис. 2.8: 8

И перезагрузим

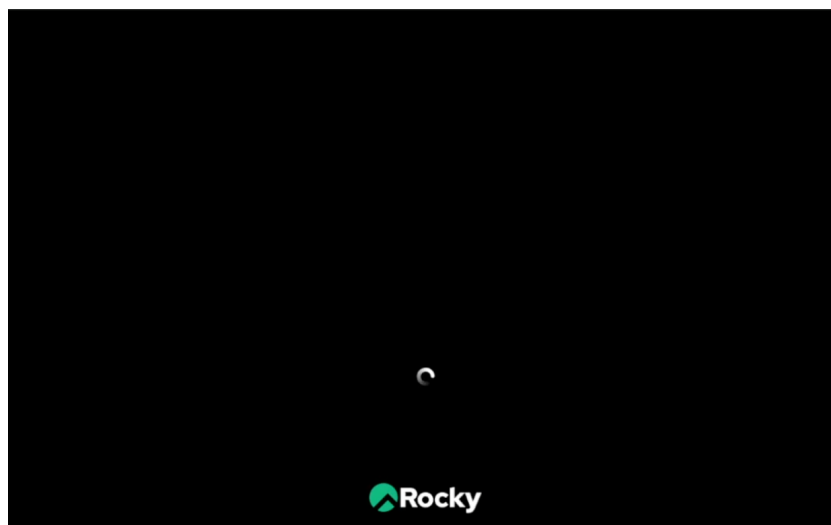


Рис. 2.9: 9

После перезагрузки посмотрим текущую информацию о состоянии SELinux командой `sestatus -v`

```
[sikaznacheev@localhost ~]$ sudo sestatus -v
[sudo] пароль для sikaznacheev:
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. 2.10: 10

Далее запускаем терминал и получаем полномочия администратора, затем просматриваем контекст безопасности файла /etc/hosts

```
[sikaznacheev@localhost ~]$ su -
Пароль:
[root@localhost ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
```

Рис. 2.11: 11

После скопируем файл /etc/hosts в домашний каталог и проверим контекст файла ~/hosts

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

Рис. 2.12: 12

Пытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc: и замет убеждаемся что тип контекста по-прежнему установлен на admin_home_t

```
[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
```

Рис. 2.13: 13

Далее исправляем контекст безопасности

```
[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
```

Рис. 2.14: 14

Убеждаемся что тип контекста изменился и вводим touch /.autorelabel для массового исправления контекста безопасности

```
[root@localhost ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@localhost ~]# touch /.autorelabel
```

Рис. 2.15: 15

Перезагружаем систему и во время перезагрузки нажимаем клавишу esc

```
Mounting Kernel Configuration File System...
Starting Flash Journal to Persistent Storage...
Starting Load/Save OS Random Seed...
Starting Create Static Device Nodes in /dev...
OK ] Finished Load Kernel Modules.
OK ] Finished Generate network units from Kernel command line.
OK ] Finished Coldplug all udev devices.
OK ] Mounted FUSE Control File System.
OK ] Mounted Kernel Configuration File System.
OK ] Reached target: Preparation for Network.
Starting Apply Kernel Variables...
Starting Wait for udev To Complete Device Initialization...
OK ] Finished Load/Save OS Random Seed.
OK ] Finished Apply Kernel Variables.
OK ] Finished Monitoring of LVM2 mirrors, snapshots etc. using dmccoutd or progress polling.
Starting Basic System.
Starting File-based Manager for Device Events and Files...
OK ] Finished Flash Journal to Persistent Storage.
OK ] Started File-based Manager for Device Events and Files.
Starting Load Kernel Module configs...
Starting Load Kernel Module fuse...
OK ] Finished Load Kernel Module configs.
OK ] Finished Load Kernel Module fuse.
OK ] Started /usr/sbin/lsnchange -say --autoactivation event pl.
OK ] Finished Wait for udev To Complete Device Initialization.
Starting Load Kernel Module efi_gstore...
OK ] Reached target: Preparation for Local File Systems.
Mounting /boot...
OK ] Finished Load Kernel Module efi_gstore.
OK ] Mounted /boot.
OK ] Reached target: Local File System.
Starting Tell Plymouth To Write Out Runtime Data...
Starting Automatic Boot Loader Update...
Starting Create Volatile Files and Directories...
OK ] Finished Automatic Boot Loader Update.
OK ] Finished Tell Plymouth To Write Out Runtime Data.
OK ] Finished Create Volatile Files and Directories.
Starting Record System Boot/Shutdown in UTMP...
OK ] Finished Record System Boot/Shutdown in UTMP.
OK ] Reached target: System Initialization.
OK ] Started Manage Sound Card State (restore and store).
OK ] Reached target: Sound Card.
Starting Restore /run/initramfs on shutdown...
Starting Relabel all filesystems...
OK ] Finished Restore /run/initramfs on shutdown.
11.379247] selinux-autorelabel(1043): == Warning == SELinux targeted policy relabel is required.
11.379257] selinux-autorelabel(1043): == Relabeling could take a very long time, depending on file
11.379290] selinux-autorelabel(1043): == system size and speed of hard drives.
11.387197] selinux-autorelabel(1043): Running: /sbin/tidfiles -T 0 restore
```

Рис. 2.16: 16

После чего переходим в супер пользователя и устанавливаем пакет httpd

```

[isikaznacheev@localhost ~]$ su -
Пароль:
[root@localhost ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64                32 kB/s | 7.9 kB  00:00
Extra Packages for Enterprise Linux 9 - x86_64                391 kB/s | 20 MB  00:52
Rocky Linux 9 - BaseOS                                         5.1 kB/s | 4.1 kB  00:00
Rocky Linux 9 - AppStream                                       5.2 kB/s | 4.5 kB  00:00
Rocky Linux 9 - Extras                                         2.7 kB/s | 2.9 kB  00:01
Пакет httpd-2.4.62-4.el9_6.4.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.

```

Рис. 2.17: 17

И устанавливаем пакет lynx

```

[root@localhost ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:45 назад, Пт 24 окт 2025 13:59:36.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий      Размер
-----
Установка:
lynx      x86_64       2.8.9-20.el9      appstream         1.5 М
=====
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                930 kB/s | 1.5 MB  00:01
-----
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          1/1
Запуск скрипглета: lynx-2.8.9-20.el9.x86_64  1/1
Проверка : lynx-2.8.9-20.el9.x86_64          1/1
Установлен:
lynx-2.8.9-20.el9.x86_64
Выполнено!

```

Рис. 2.18: 18

Далее создаем папку под названием web и переходим в нее и создаем в ней файл index.html

```

[root@localhost ~]# mkdir /web
[root@localhost ~]# cd /web
[root@localhost web]# touch index.html

```

Рис. 2.19: 19

Затем открываем файл index.html и записываем следующее

```

GNU nano 5.6.1 index.html
welcome to my web-server

```

Рис. 2.20: 20

После в файле /etc/httpd/conf/httpd.conf закоментируем строки которые указаны в лабораторной работе и заменим их

```
#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>
```

Рис. 2.21: 21

Затем запустим веб-сервер и службу httpd

```
[root@localhost web]# systemctl start httpd
[root@localhost web]# systemctl enable httpd
```

Рис. 2.22: 22

Далее в терминале под учетной записью пользователя обратимся к веб серверу в текстовом браузере lynx:

```
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. 2.23: 23

Затем в терминале с полномочиями администратора применим новую метку

контекста к /web и восстановим контекст безопасности

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

Рис. 2.24: 24

И пробуем снова обратиться к веб-серверу и увидим Welcome to my web-server

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

Рис. 2.25: 25

После всех проделанных действий запускаем терминал и получаем полномочия администратора и просматриваем список переключателей SELinux для службы ftp

```
[root@localhost ~]# 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@localhost ~]#
```

Рис. 2.26: 26

Для службы ftpd_anon посмотрим список переключателей мы увидим что система настроена безопасно-анонимная запись через ftp запрещена это стандартная и рекомендуемая конфигурация для большинства сценариев использования ftp-сервера

```
[root@localhost ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
```

Рис. 2.27: 27

После изменяем текущее значение переключателей для службы ftpd_anon_write с off на on и повторно просматриваем список переключателей SELinux для службы ftpd_anon_write

```
[root@localhost ~]# setsebool ftpd_anon_write on
[root@localhost ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
```

Рис. 2.28: 28

После просмторим список переключателей первая команда для просмотра всех boolean-переключателей с фильтром по ftpd_anon затем изменяем постоянное значение переключателей для службы tpd_anon_write с off на on и просматриваем список переключателей и последняя команда для просмотра всех boolean-переключателей с фильтром по ftpd_anon

```
[root@localhost ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
[root@localhost ~]# setsebool -P ftpd_anon_write on
[root@localhost ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@localhost ~]#
```

Рис. 2.29: 29

3 Контрольные вопросы

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

Ответ - временный permissive- режим `setenforce 0`

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

Ответ - список переключателей `getsebool -a`

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

Ответ - пакет для читаемых сообщений SELinux `setroubleshoot`

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

Ответ - надо применить тип `httpd_sys_content_t` к `/web`

Команды `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)"?` и `restorecon -Rv /web`

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

Ответ - полное отключение SELinux -редактировать `/etc/selinux/config`

6. Где SELinux регистрирует все свои сообщения?

Ответ - логи SELinux /var/log/audit/audit.log

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

Ответ - узнать доступные контексты для ftp semanage fcontext -l | 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?

Ответ - командой setenforce 0

4 Вывод

После выполнения лабораторной работы я получил навыки работы с контекстом безопасности и политиками SELinux