

# **Отчет о лабораторной работе**

**Лабораторная работа №9**

Казначеев Сергей Ильич

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение лабораторной работы</b>	<b>6</b>
<b>3 Контрольные вопросы</b>	<b>16</b>
<b>4 Вывод</b>	<b>18</b>

# 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).

```
[sikaznacheev@localhost ~]$ su -  
Пароль:
```

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

сти Стока 12 - Ядро поддерживает политики SELinux до версии 33 включительно  
Строка 14 - начало раздела с контекстами безопасности текущих процессов Странка 15 - Текущая сессия пользователя работает в неограниченном домене сам домен Странка 16 - Основной системный процесс init работает в домене init\_t Странка 17 - Домен ssh работает в ограниченном домене sshd\_t с дополнительными уровнями безопасности Странка 19 - начало раздела с контекстами безопасности системных файлов Странка 20 - Управляющий терминал имеет тип user\_devpts\_t для псевдо терминалов Странка 21 - Файл с учетными записями пользователей имеет тип passwd\_file\_t Странка 22 - файл с хешами паролей имеет защищенный тип shadow\_t Странка 23 - Исполняемый файл bash имеет тип shell\_exec\_t Странка 24 - Исполняемый файл login bvttn nbg login\_exec\_t Странка 25 - Символическая ссылка /bin/sh указывает на файл с типом shell\_exec\_t Странка 26 - Исполняемый файл getty имеет тип getty\_exec\_t Странка 27 - исполняемый файл init имеет тип init\_exec\_t Странка 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
/sbin/getty                          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 просмотрим 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 просмотрим 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 pro
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Рис. 2.8: 8

И перезагрузим

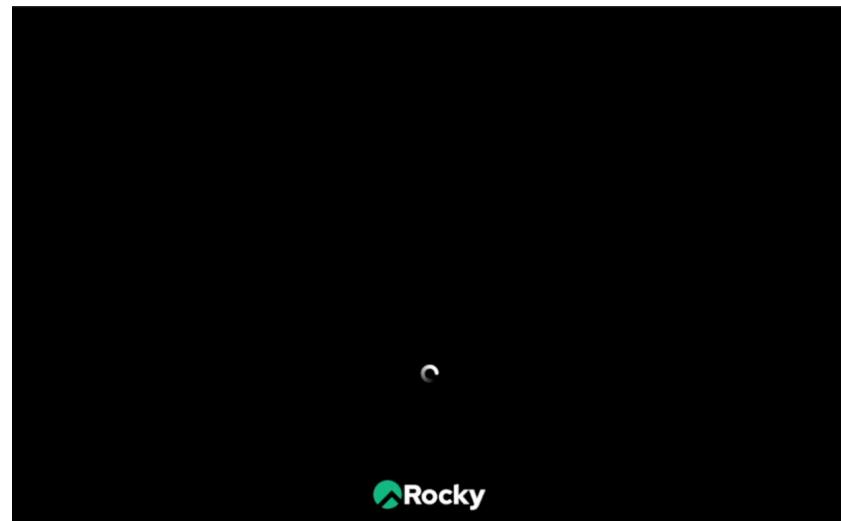


Рис. 2.9: 9

После перезагрузки просмотрим 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  
[root@localhost ~]#
```

Рис. 2.15: 15

Перезагружаем систему и во время перезагрузки нажимаем клавишу esc

```
Starting kernel Log Initialization File System...  
Starting Kernel Module 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 Collect All Network Interfaces.  
[ OK ] Mounted FUSE Control File System.  
[ OK ] Mounted Kernel Configuration File System.  
[ OK ] Reached target Preparation For Network.  
Starting Kernel Module 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 dmevent or progress polling.  
[ OK ] Started udevd.  
Starting Rule-based Manager for Device Events and Files...  
[ OK ] Finished Flush Journal to Persistent Storage.  
[ OK ] Started Rule-based Manager for Device Events and Files.  
Starting Kernel Module Udevd Udevd...  
Starting Load Kernel Module fuse.  
[ OK ] Finished Load Kernel Module configs.  
[ OK ] Finished Load Kernel Module fuse.  
[ OK ] Started /var/lib/udev/rules.d/70-persistent-net.rules --activation event r.  
[ OK ] Started udevd.service To Complete Device Initialization.  
Starting Load Kernel Module efi_gptstore...  
[ OK ] Reached target Preparation for Local File Systems.  
Mounting /boot...  
[ OK ] Mounted /boot.  
[ OK ] Mounted /Kernel Module efi_gptstore.  
[ OK ] Mounted /host.  
[ OK ] Reached target Local File Systems.  
Starting Tell Plymouth To Write Out Runtime Data...  
Starting Automatic Root Loader Update...  
Starting Create UefiTable Files Directories...  
[ OK ] Finished automatic Root Loader Update.  
[ OK ] Finished Tell Plymouth To Write Out Runtime Data.  
[ OK ] Finished Create Volatile Files and Directories.  
[ OK ] Finished Record System Boot/Shutdown in UDEV...  
[ OK ] Reached target System Initialization.  
[ OK ] Started Manage Sound Card State (restore and store).  
[ OK ] Reached target Sound Cards.  
Starting Stop /run/initramfs's on shutdown...  
Starting Relabel all filesystems...  
[ OK ] Finished Restart /run/initramfs's on shutdown.  
11.379247] selinux-autorelabel[0x43]: *** Warning -- SELinux targeted policy relabel is required.  
11.379247] selinux-autorelabel[0x43]: *** This may take some time, depending on file size.  
11.379280] selinux-autorelabel[0x43]: *** system size and speed of hard drives.  
11.367197] selinux-autorelabel[0x43]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2.16: 16

После чего переходим в супер пользователя и устанавливаем пакет httpd

```
[sikaznacheev@localhost ~]$ su -
Пароль:
[root@localhost ~]# dnf -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64
Extra Packages for Enterprise Linux 9 - x86_64
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
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          797 kB/s | 1.5 MB   00:01
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакций проведен успешно.
Выполнение транзакции
Подготовка   : 1/1
Установка    : lynx-2.8.9-20.el9.x86_64 1/1
Запуск скриптилета: 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 5.1
index.html
Изменён
Welcome to my web-server.
```

Рис. 2.20: 20

После в файле /etc/httpd/conf/httpd.conf закоменитирам 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:

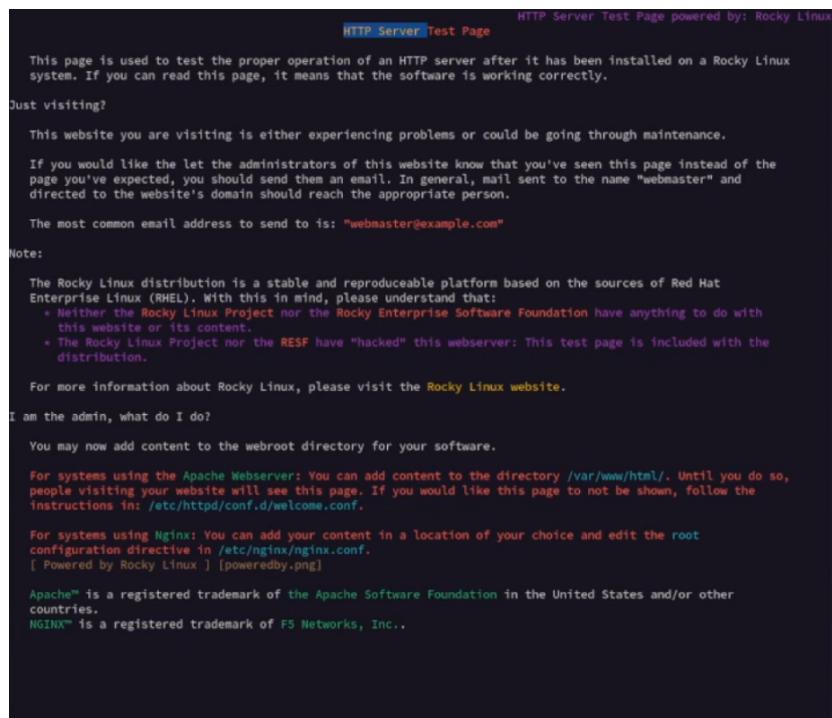


Рис. 2.23: 23

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

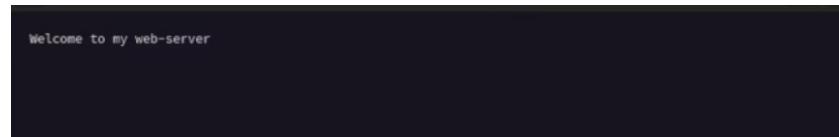


Рис. 2.25: 25

После всех прооделанных 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 просмотрим 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 просмотрим 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., вкл.) 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
```

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