Управление SELinux

Лабораторная работа №9

Казначеев С.И.

24 октября 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

:::::::::::::: {.columns align=center} ::: {.column width="70%"}

- Казначеев Сергей Ильич
- Студент
- Российский университет дружбы народов
- [1132240693@pfur.ru] ::: ::: {.column width="30%"}

Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

Для начала откроем терминал и перейдем в супер пользователя

Рис. 1: 1

Посмотрим текущую информации

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

Отдельно описание

1. • пользователь то есть я на хосте localhost выполнил команду sestatus -v с правами суперпользователя
2. • запрос пароля sudo система запросила пароль пользователя для предоставления прав суперпользователя
3. • Общий статус SELinux был активирован в системе и функционирует
4. • Виртуальная файловая система SELinux смонтирована в директории через эту файловую систему ядро предоставляет информацию о SELinux
5. = основные конфигурациионные файлы и политики SELinux расположены в директории /etc/selinux
6. • Загружена политика безопасноти типа targeted - защищаются только определенные системные службы остальные процессы работают без ограниченний

Отдельно описание

7. • SELinux работает в режиме принудительного применения политики - все нарушения блокируются
8. • Режим enforcing установлен в концигурационном фалйе и будет сохраняться после перезагрузки
9. • поддержка Multi-level Security включена в политику
10. • Политика разрешает доступ к объектам с неизвестными классами или разрешениями
11. • SELinux проверяет защиту памяти на основе фактических безопасности
12. • Ядро поддерживает политики SELinux до версии 33 включительно

Отдельно описание

- начало раздела с контекстами безопасности текущих процессов
- Текущая сессия пользователя работает в неограниченном домене сам домен
- Основной системный процесс init работает в домене init_t
- Домен ssh работает в ограниченном домене sshd_t с дополнительными уровнями безопасности
- начало раздела с контекстами безопасности системных файлов
- Управляющий терминал имеет тип user_devpts_t для псевдо терминалов
- Файл с учетными записями пользователей имеет тип passwd_file_t
- файл с хешами паролей имеет защищенный тип shadow_t
- Исполняемый файл bash имеет тип shell_exec_t
- Исполняемый файл login bvttn nbg login_exect_t
- Символичная ссылка /bin/sh указывает на файл с типом shell_exec_t
- Исполяемый файл agetty имеет тип getty_exec_t
- исполняемый файл init имеет тип init_exec_t
- Исполняемый файл ssh домена имеет тип ssh_exec_t

Скрин

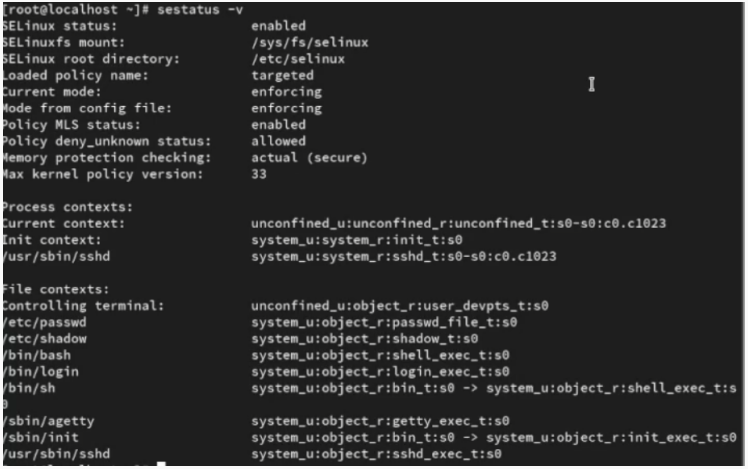

[root@localhost ~]# sestatus -v
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: 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:s
0
/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

Просмотрим в какома режиме работает SELinux

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

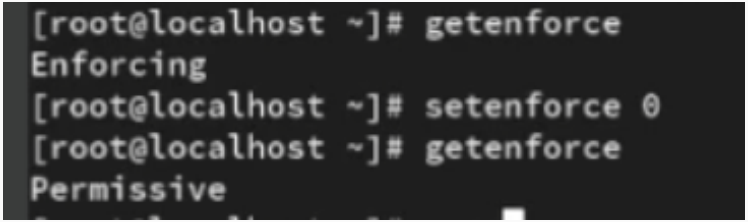


Рис. 3: 3

Запись в файл

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

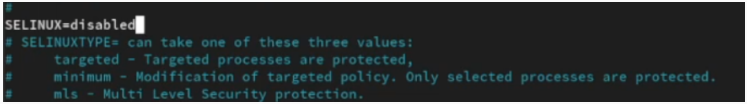


Рис. 4: 4

Перезагрузка системы

Перезагрузим систему

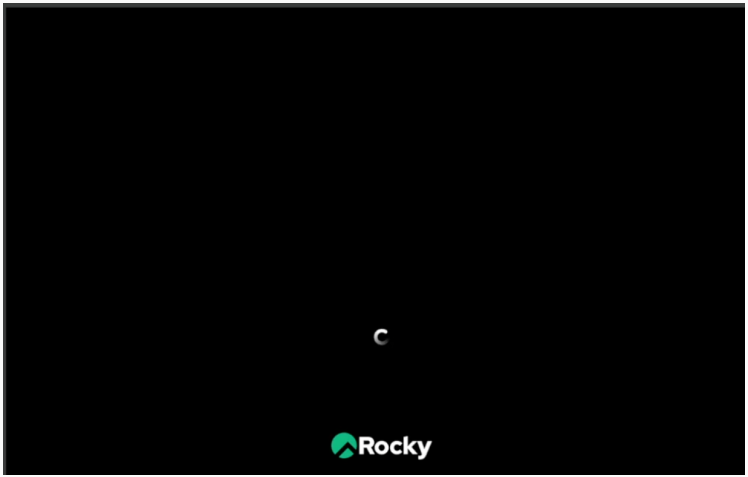


Рис. 5: 5

Проверка статуса после перезагрузки

После перезагрузки просмотрим статуст SELinux

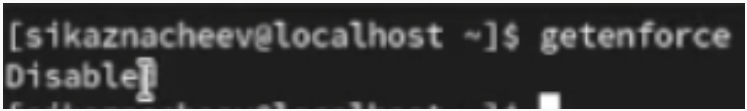


Рис. 6: 6

Затем пробуем переключить режим работы SELinux

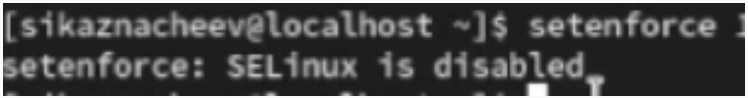


Рис. 7: 7

Меняем занчение

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

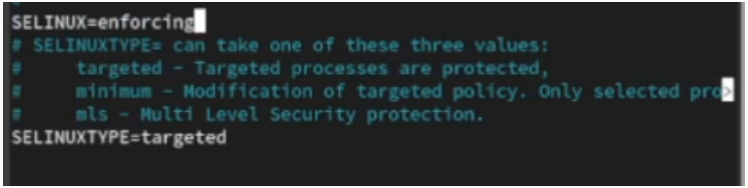


Рис. 8: 8

И перезагрузим

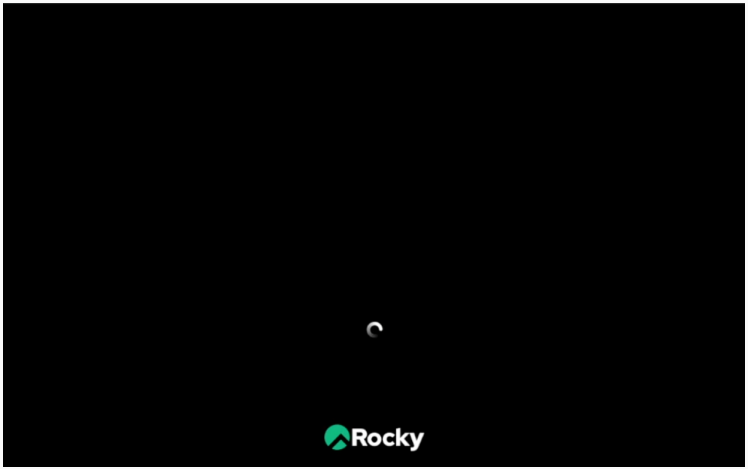
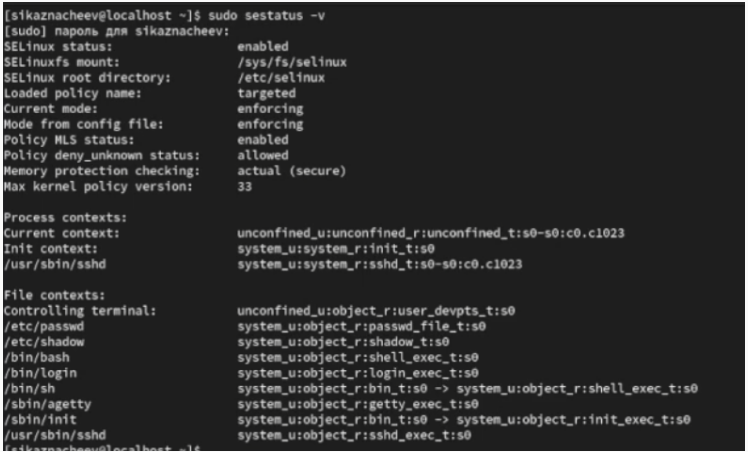


Рис. 9: 9

Просмотр текущей информации

После перезагрузки просмотрим текущую информацию о состоянии SELinux командой sestatus -v



Далее запускаем терминал и получаем полномочия администратора, затем просмотриваем контекст безопасноти файла /etc/hosts

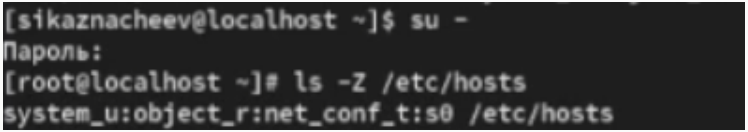


Рис. 11: 11

Копирование файла

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. 12: 12

Перезаписываем файл

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

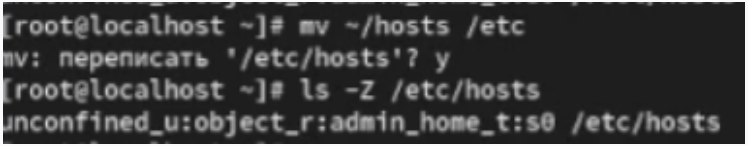


Рис. 13: 13

Исправляем контекст безопасности

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. 14: 14

Убеждаемся что тип контекста изменился

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

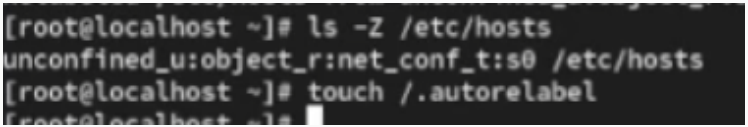


Рис. 15: 15

Перезагружаем систему и во время перезагрузки нажимаем клавишу esc

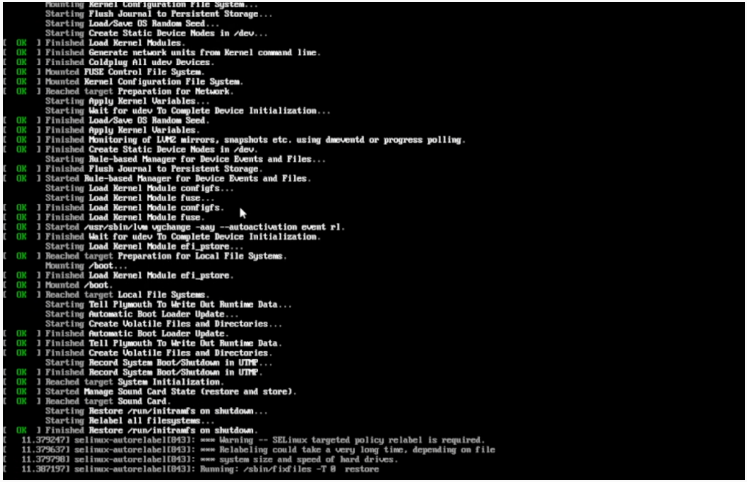


Рис. 16: 16

Устанавливаем пакет httpd

После чего переходим в супер польователя и устанавливаем пакет httpd

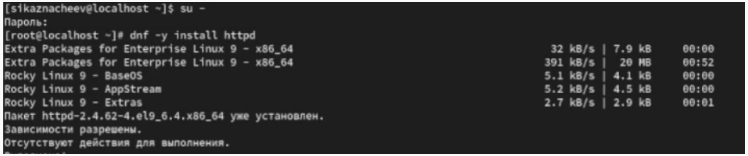


Рис. 17: 17

И устанавливаем пакет lynx

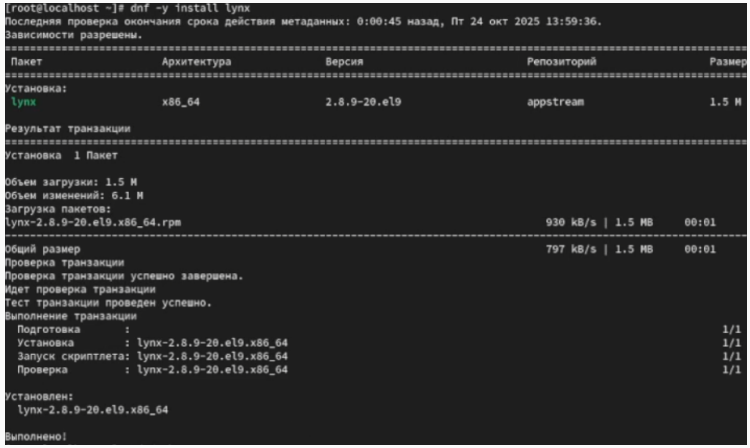


Рис. 18: 18

Создаем папку под названием web

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. 19: 19

Открываем файл index.html

Затем открываем файл index.html и записываем следующее

Рис. 20: 20

Изменяем файл

После в файле /etc/httpd/conf/httpd.conf закоменнтираем строки которые указаны в лабораторной работае и заменим их

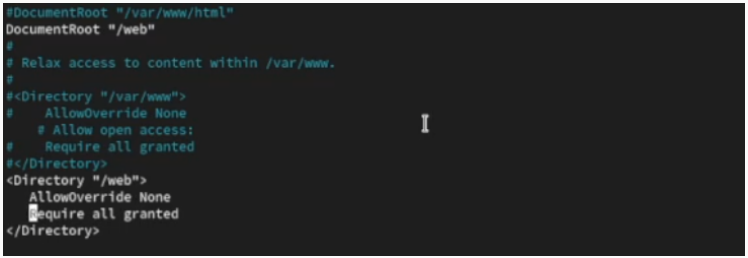


Рис. 21: 21

Запустим веб-сервер

Затем запустим веб-сервер и службу httpd

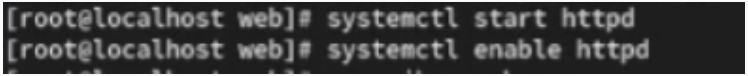
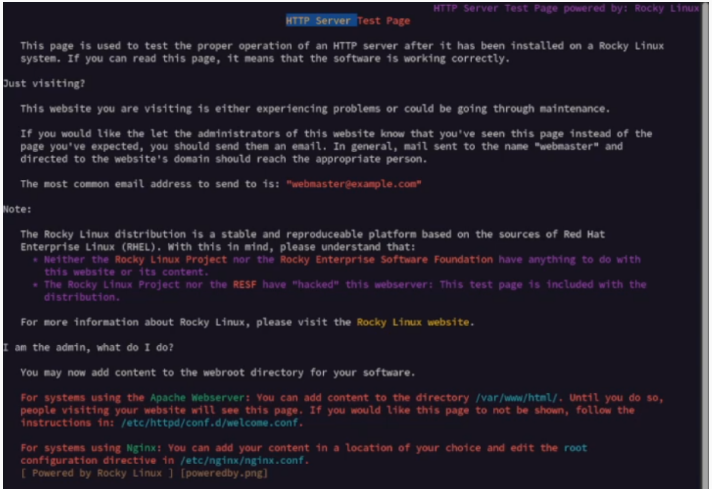


Рис. 22: 22

Запустим веб-сервер в текстовом браузере lynx

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



Применим новую метку контекста к /web

Затем в терминале с полномочиями администратора применим новую метку контекста к /web и восстановим контекст безопасности

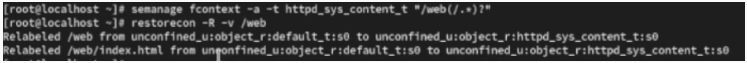


Рис. 24: 24

Пробуем снова обратиться к веб-серверу

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

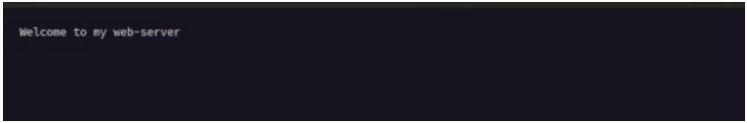


Рис. 25: 25

Просмотр списков переключателей SELinux для службы ftp

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. 26: 26

Просмотр списков переключателей

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

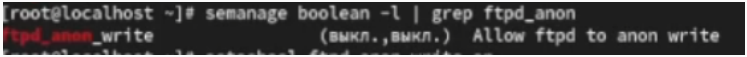


Рис. 27: 27

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

Рис. 28: 28

Просмотр списков переключателей

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

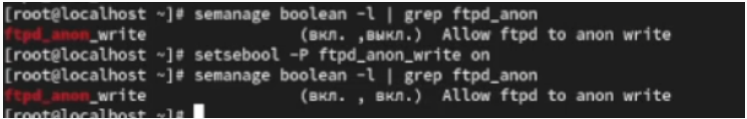


Рис. 29: 29

Контрольные вопрос 1

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

Ответ - временный permissive- режим setenforce 0

Контрольные вопрос 2

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

Ответ - список переключателей getsebool -a

Контрольные вопрос 3

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

Ответ - пакет для читаемых сообщений SELinux setroubleshoot

Контрольные вопрос 4

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

Контрольные вопрос 5

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

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

Контрольные вопрос 6

6. Где SELinux регистрирует все свои сообщения?

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

Контрольные вопрос 7

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

Контрольные вопрос 8

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

Вывод

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