Отчёт по лабораторной работе №9. Управление SELinux

Дисциплина: Основы администрирование операционных систем

Жукова Арина Александровна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux. # Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов вебслужбы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

2 Выполнение лабораторной работы

2.1 Управление режимами SELinux

1. Запустила терминал и получила полномочия администратора. Просмотрела текущую информацию о состоянии SELinux: `sestatus -v` (рис.2.1).

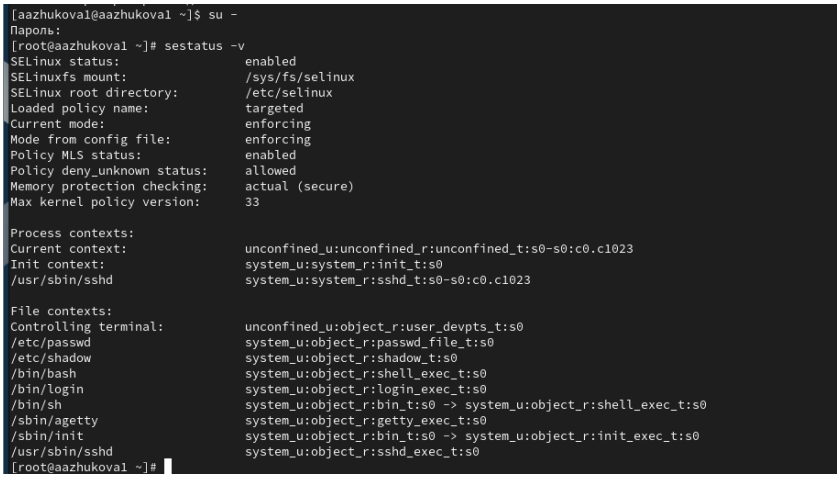

Рис. 2.1: Просмотр текущей информации

2. Посмотрела, в каком режиме работает SELinux: `getenforce`. По умолчанию SELinux находился в режиме принудительного исполнения (Enforcing). Изменила режим работы SELinux на разрешающий (Permissive) (рис. 2.2).

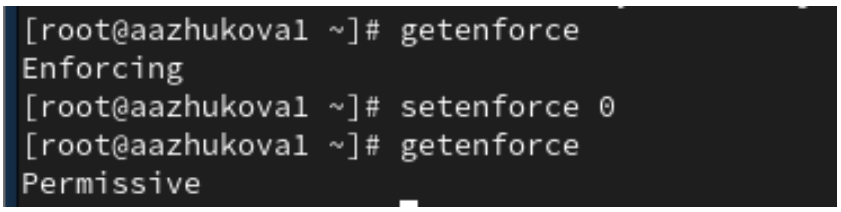

Рис. 2.2: Просмотр режима, изменение режима

3. В файле /etc/sysconfig/selinux с помощью редактора установила: `SELINUX=disabled`. Перезагрузила систему. После перезагрузки запустила терминал и получила полномочия администратора. Посмотрела статус SELinux. Попробовала переключить режим работы SELinux: `setenforce 1` (рис. 2.3).

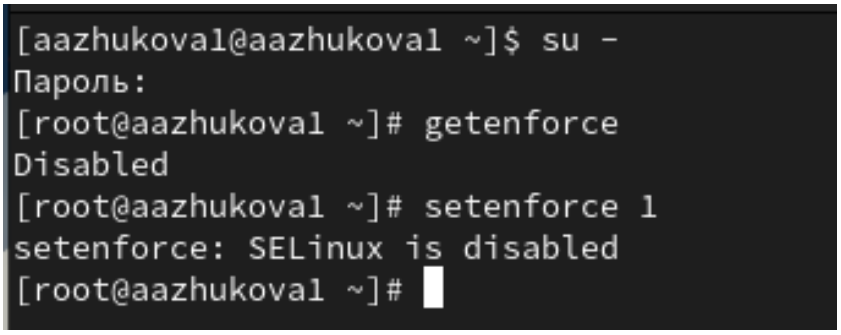

Рис. 2.3: Изменение статуса с помощью редактора

Не могла переключаться между отключённым и принудительным режимом без перезагрузки системы.

4. Открыла файл /etc/sysconfig/selinux с помощью редактора и установила: `SELINUX=enforcing`. Перезагрузила систему. После перезагрузки в терминале с полномочиями администратора просмотрела текущую информацию о состоянии SELinux: `sestatus -v`. Убедилась, что система работает в принудительном режиме (enforcing) использования SELinux (рис. 2.4).

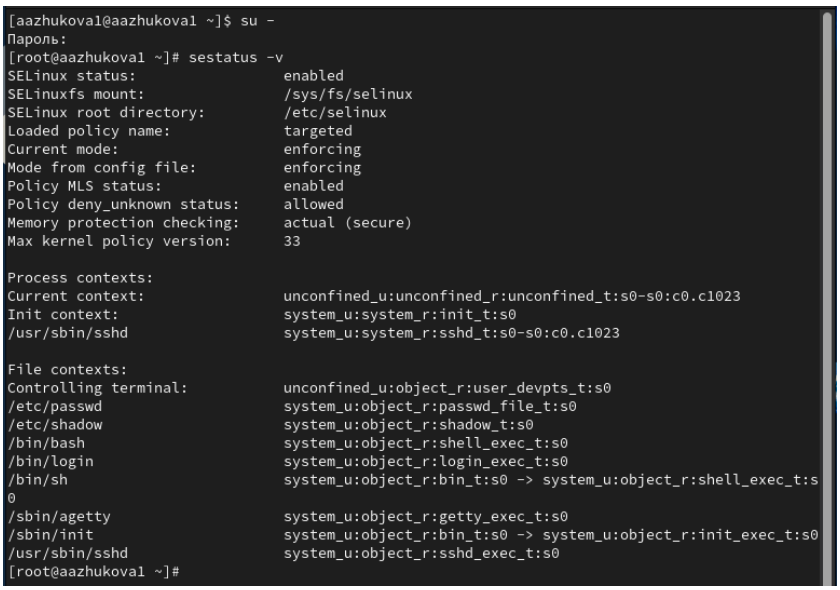

Рис. 2.4: Установка принудительного режима

2.2 Использование restorecon для восстановления контекста безопасности

1. Запустила терминал и получила полномочия администратора. Посмотрела контекст безопасности файла /etc/hosts: `ls -Z /etc/hosts`. Увидела, что у файла есть метка контекста net_conf_t. Скопировала файл /etc/hosts в домашний каталог Проверила контекст файла ~/hosts. Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, стал admin_home_t. Попыталась перезаписать существующий файл hosts из домашнего каталога в каталог /etc. Убедилась, что тип контекста по-прежнему установлен на admin_home_t (рис. 2.5).

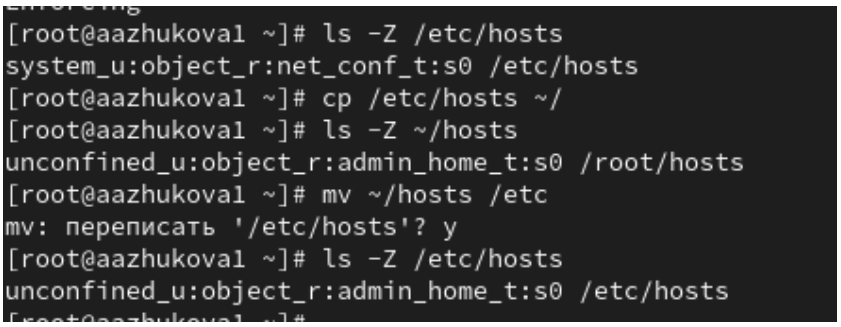

Рис. 2.5: Просмотр контекста безопасности файла, копирование файла, перезапись существующего файла

2. Исправила контекст безопасности `restorecon -v /etc/hosts`. Опция -v показала процесс изменения. Убедилась, что тип контекста изменился. Для массового исправления контекста безопасности на файловой системе ввела: `touch /.autorelabel` (рис. 2.6).

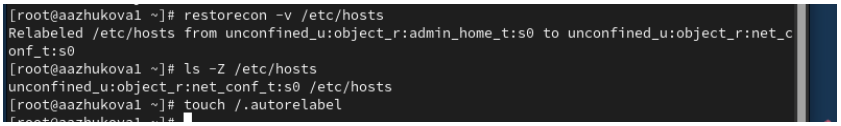

Рис. 2.6: Исправление контекста безопасности, массовое исправление контекста

и перезагрузила систему. Во время перезапуска не забыла нажать клавишу Esc на клавиатуре, чтобы видела загрузочные сообщения. Увидела, что файловая система автоматически перемаркирована.

2.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запустила терминал и получила полномочия администратора. Установила необходимое программное обеспечение: `httpd` и `lynx` (рис. 2.7).

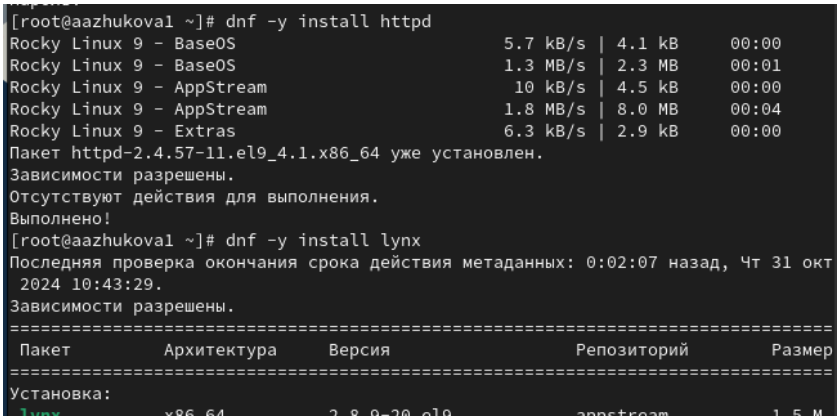

Рис. 2.7: Установка программного обеспечения

2. Создала новое хранилище для файлов веб-сервера. Создала файл index.html в каталоге с контентом веб-сервера (рис. 2.8).

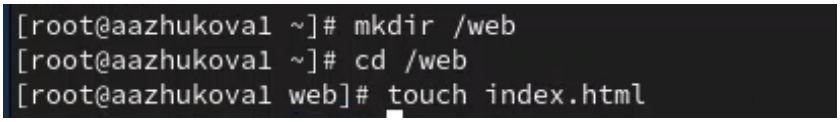

Рис. 2.8: Создание нового хранилища и файла

3. Поместила в файл следующий текст `Welcome to my web-server` (рис. 2.9).

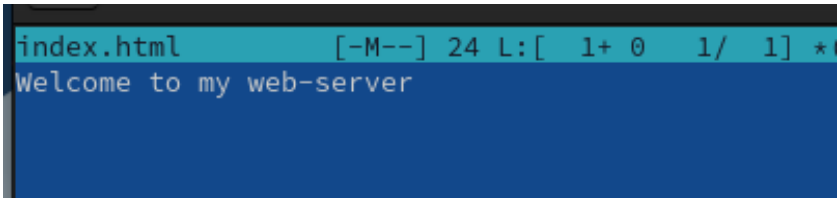

Рис. 2.9: Изменение файла

4. Внесла изменеия в файле /etc/httpd/conf/httpd.conf (рис. 2.10).

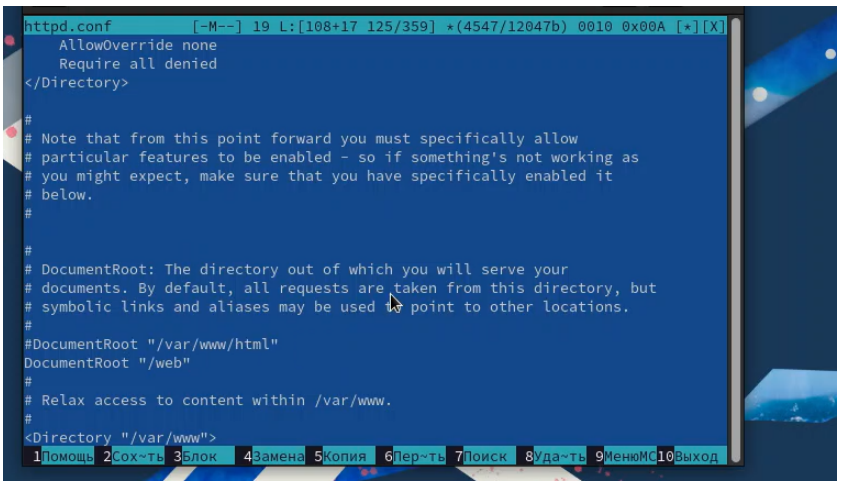

Рис. 2.10: Изменение файла

5. Запустила веб-сервер и службу httpd (рис. 2.11).

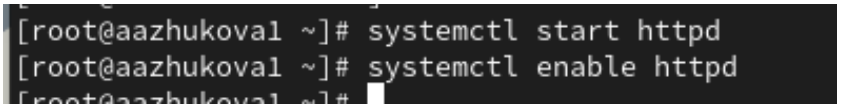

Рис. 2.11: Запуск веб сервера и службы httpd

6. В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: `lynx http://localhost` увидела веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html (рис. 2.12).

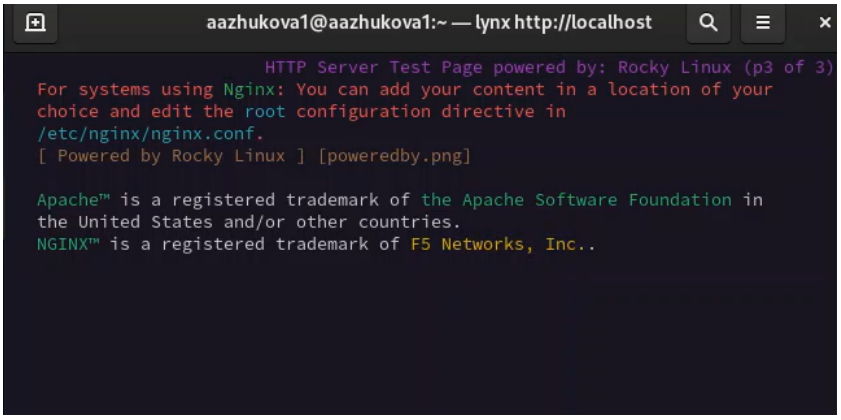

Рис. 2.12: Обращение к веб-серверу

7. В терминале с полномочиями администратора применила новую метку контекста к /web: `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`. Восстановила контекст безопасности (рис. 2.13).

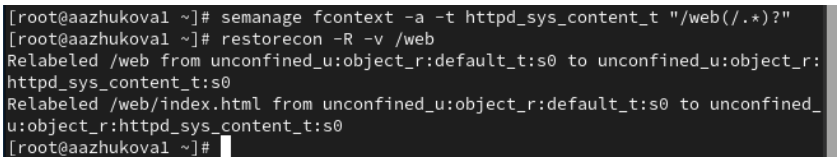

Рис. 2.13: Применение новой метки к контексту, восстановление контекста

8. В терминале под учётной записью своего пользователя снова обратилась к веб-серверу (рис. 2.14).

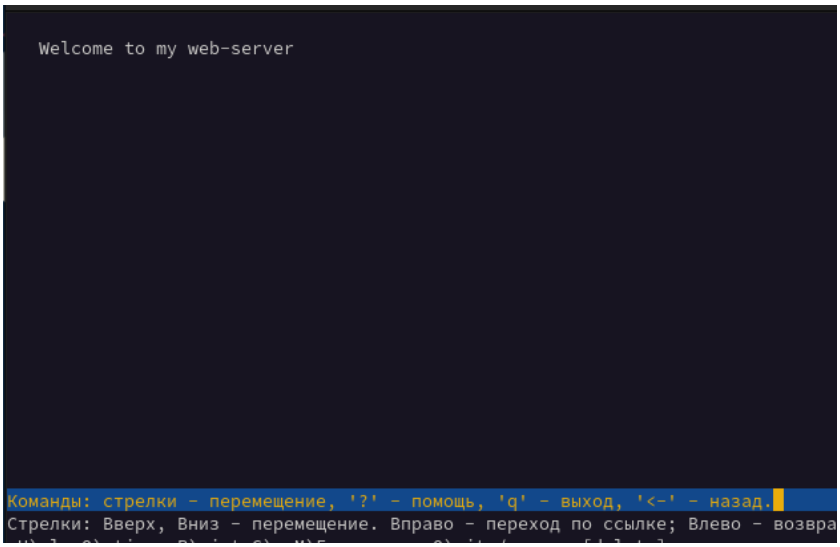

Рис. 2.14: Обращение к веб-серверу

2.4 Работа с переключателями SELinux

1. Запустила терминал и получила полномочия администратора. Посмотрела список переключателей SELinux для службы ftp: `getsebool -a | grep ftp`. Для службы ftpd_anon посмотрела список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен (рис. 2.15).

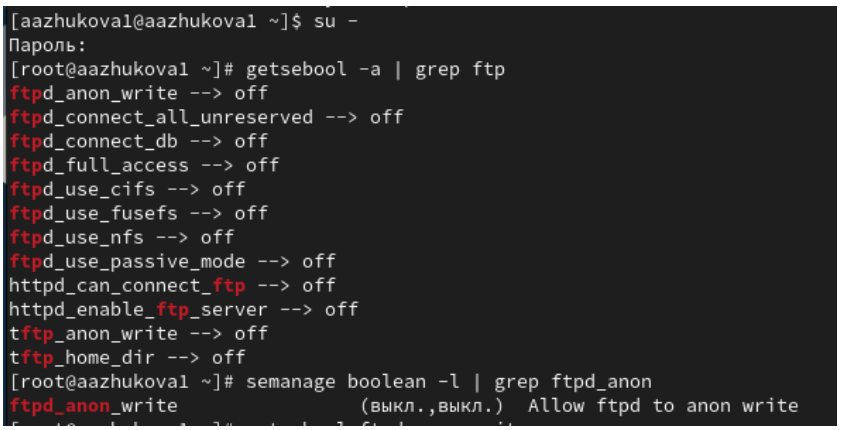

Рис. 2.15: Просмотр списка переключателей

2. Изменила текущее значение переключателя для службы ftpd_anon_write с off на on. Повторно посмотрела список переключателей SELinux для службы ftpd_anon_write. Посмотрела список переключателей с пояснением (рис. 2.16).

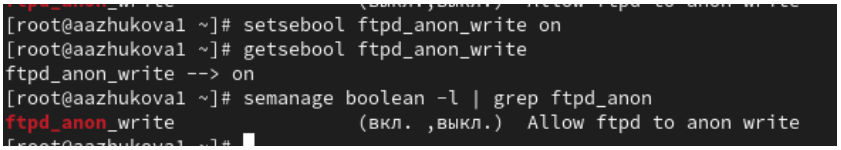

Рис. 2.16: Изменение текущего значения переключателя

Обратила внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

3. Изменила постоянное значение переключателя для службы ftpd_anon_write с off на on: `setsebool -P ftpd_anon_write on`. Посмотрела список переключателей (рис. 2.17).

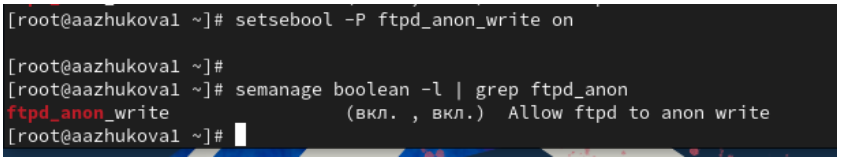

Рис. 2.17: Изменение постоянного значения переключателя

3 Ответы на контрольные вопросы

1. setenforce 0
2. getenforce
3. audit-libs-devel
4. chcon -t httpd_sys_content_t /web
5. /etc/selinux/config
6. /var/log/audit/audit.log
7. semanage fcontext -l | grep ftp
8. Проверить журнал аудита SELinux: ausearch -m avc

4 Выводы

Во время выполнения лабораторной работы я получила навыки работы с контекстом безопасности и политиками SELinux.

Список литературы

1. Mayer F., MacMillan K., Caplan D. SELinux by example: using Security Enhanced Linux. — Prentice Hall, 2006.
2. Vermeulen S. SELinux Cookbook. — Packt Publishing Ltd, 2014.
3. Vermeulen S. SELinux System Administration. — 2nd Edition. — Packt Publishing Ltd,
4.
5. Vugt S. van. Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — (Certification Guide).
6. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / M. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: https: / / docs - old . fedoraproject . org / ru - RU / Fedora / 13 / html / Security - Enhanced_Linux/index.html.