Лабораторная работа № 9

Отчёт

Ермишина Мария Кирилловна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данной лабораторной работы является получение навыков работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

1. Управление режимами SELinux Запустите терминал и получите полномочия администратора. Просмотрите текущую информацию о состоянии SELinux: (рис. 2.1)

- sestatus -v Посмотрите, в каком режиме работает SELinux: (рис. 2.1)
- getenforce Измените режим работы SELinux на разрешающий (Permissive): (рис. 2.1)
- setenforce 0 и снова введите (рис. 2.1)
- getenforce

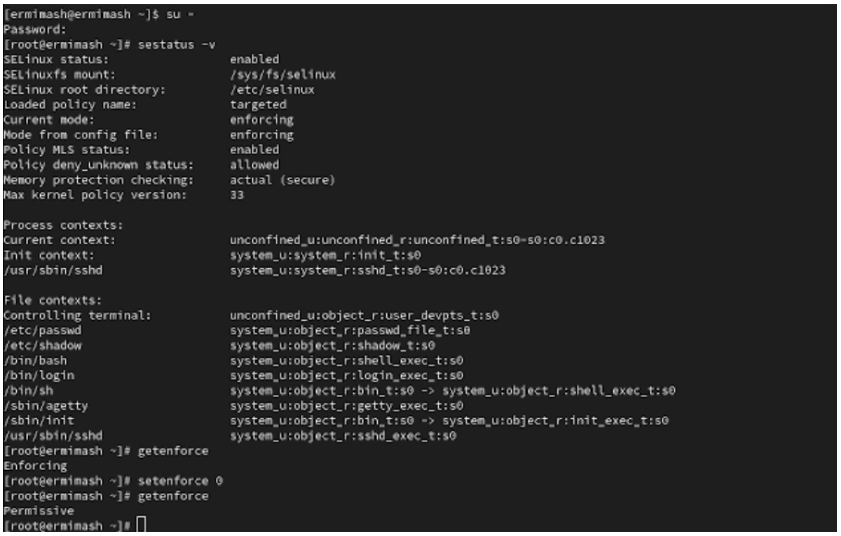

Рис. 2.1: Разрешающий режим SELinux

В файле /etc/sysconfig/selinux с помощью редактора установите: (рис. 2.2) - SELINUX=disabled

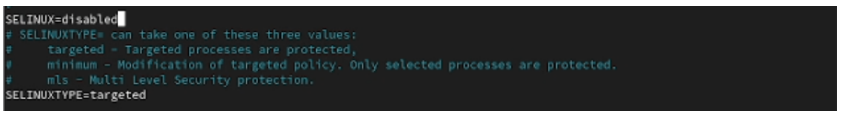

Рис. 2.2: disabled в файле SELinux

Перезагрузите систему. После перезагрузки запустите терминал и получите полномочия администратора. Посмотрите статус SELinux: - getenforce Вы увидите, что SELinux теперь отключён. Попробуйте переключить режим работы SELinux: - setenforce 1

Рис. 2.3: Проверка изменений

Откройте файл /etc/sysconfig/selinux с помощью редактора и установите: (рис. 2.4) - SELINUX=enforcing Перезагрузите систему.

Рис. 2.4: enforcing в файле SELinux

После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux: (рис. 2.5) - sestatus -v

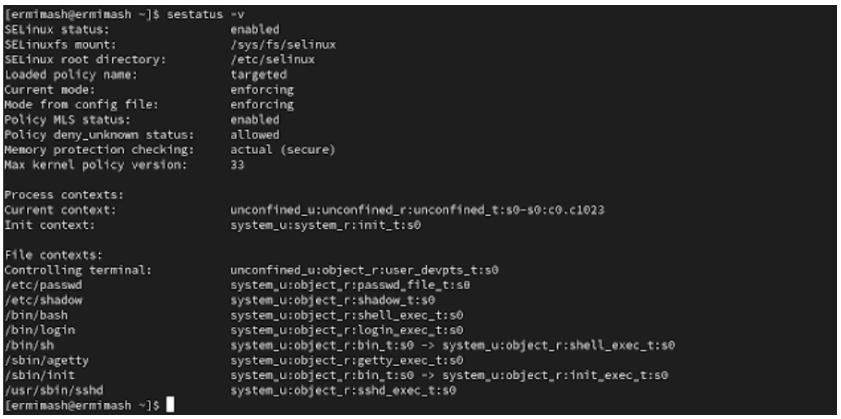

Рис. 2.5: Принудительный режим активен

2. Использование restorecon для восстановления контекста безопасности (рис. 2.6) Запустите терминал и получите полномочия администратора. Посмотрите контекст безопасности файла /etc/hosts:

- ls -Z /etc/hosts Скопируйте файл /etc/hosts в домашний каталог:
- cp /etc/hosts ~/ Проверьте контекст файла ~/hosts:
- ls -Z ~/hosts Поскольку копирование считается созданием нового файла, то параметр контекста в файле ~/hosts, расположенном в домашнем каталоге, станет admin_home_t. Попытайтесь перезаписать существующий файл hosts из домашнего каталога в каталог /etc:
- mv ~/hosts /etc Убедитесь, что тип контекста по-прежнему установлен на admin_home_t:
- ls -Z /etc/hosts Исправьте контекст безопасности:
- restorecon -v /etc/hosts Убедитесь, что тип контекста изменился:
- ls -Z /etc/hosts Для массового исправления контекста безопасности на файловой системе введите
- touch /.autorelabel

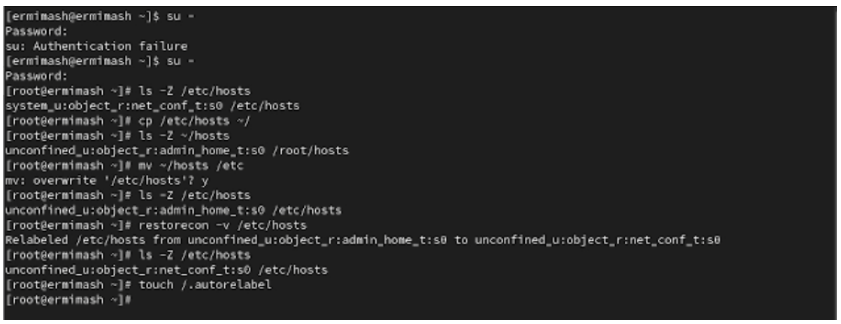

Рис. 2.6: Использование restorecon

3. Настройка контекста безопасности для нестандартного расположения файлов веб-сервера Запустите терминал и получите полномочия администратора. Установите необходимое программное обеспечение: (рис. 2.7)

- dnf -y install httpd

- dnf -y install lynx Создайте новое хранилище для файлов web-сервера: (рис. 2.7)
- mkdir /web Создайте файл index.html в каталоге с контентом веб-сервера: (рис. 2.7)
- cd /web
- touch index.html и поместите в файл следующий текст “Welcome to my web-server”

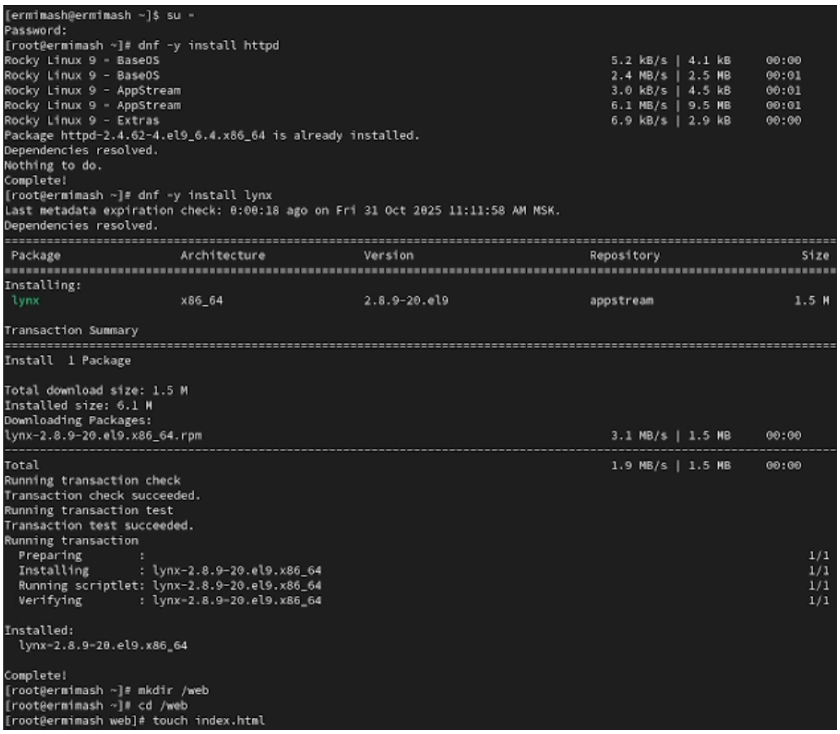

Рис. 2.7: Установка прог. обеспеч.

В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot “/var/www/html” и ниже добавьте строку “DocumentRoot”/web”” (рис. 2.8) Затем в этом же файле ниже закомментируйте раздел: (рис. 2.8) <Directory “/var/www”> AllowOverride None Require all granted и добавьте следующий раздел, определяющий правила доступа: (рис. 2.8) <Directory “/web”> AllowOverride None Require all granted

Рис. 2.8: Редакция текстового файла

Запустите веб-сервер и службу httpd: (рис. 2.10) - systemctl start httpd - systemctl enable httpd В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: (рис. 2.9) - lynx http://localhost

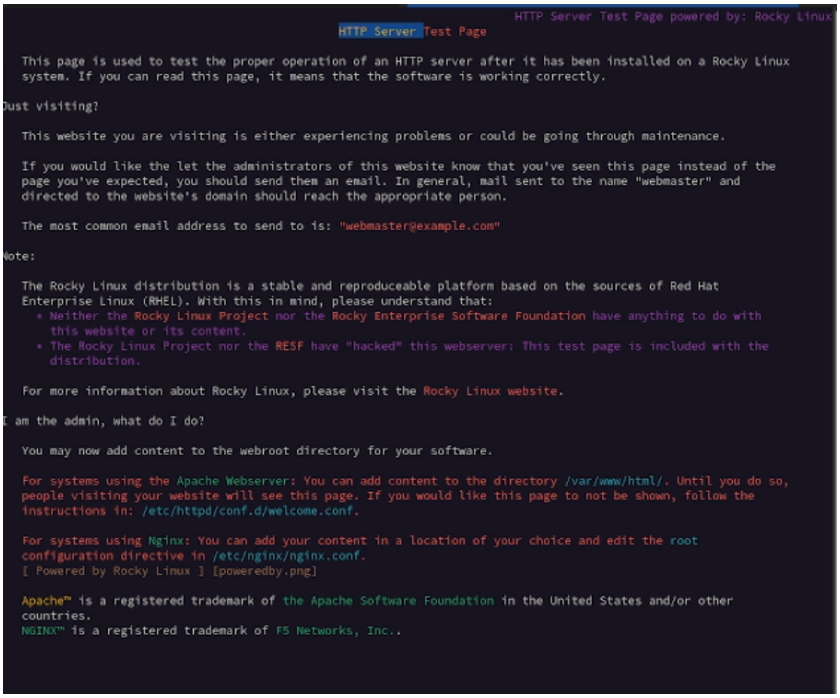

Рис. 2.9: Первый запуск сайта

В терминале с полномочиями администратора примените новую метку контекста к /web: (рис. 2.10) - semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?” Восстановите контекст безопасности: (рис. 2.10) - restorecon -R -v /web

Рис. 2.10: Восстановка контекста безопасности

В терминале под учётной записью своего пользователя снова обратитесь к веб-серверу: (рис. 2.11) - lynx http://localhost

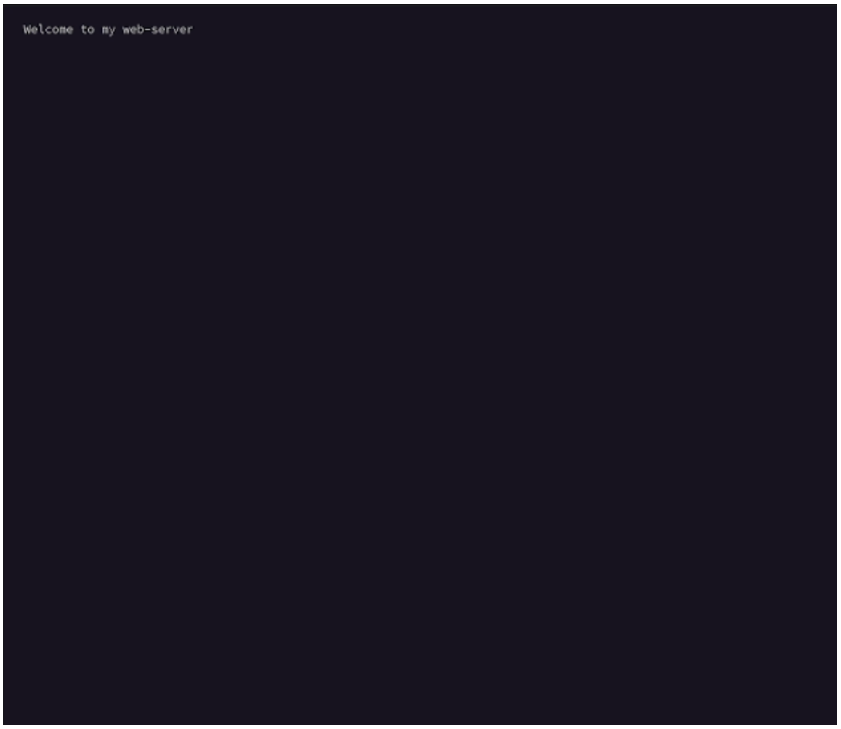

Рис. 2.11: Второй запуск

4. Работа с переключателями SELinux Запустите терминал и получите полномочия администратора. Посмотрите список переключателей SELinux для службы ftp:

- getsebool -a | grep ftp Для службы ftpd_anon посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен:
- semanage boolean -l | grep ftpd_anon Измените текущее значение переключателя для службы ftpd_anon_write с off на on:

- setsebool ftpd_anon_write on Повторно посмотрите список переключателей SELinux для службы ftpd_anon_write:
- getsebool ftpd_anon_write Посмотрите список переключателей с пояснением:
- semanage boolean -l | grep ftpd_anon Измените постоянное значение переключателя для службы ftpd_anon_write с off на on:
- setsebool -P ftpd_anon_write on Посмотрите список переключателей:
- semanage boolean -l | grep ftpd_anon

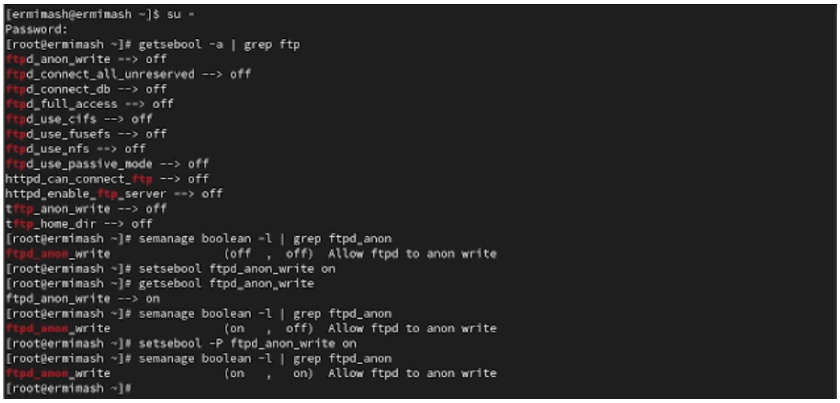

Рис. 2.12: Работа с переключателями SELinux

3 Контрольные вопросы

1. setenforce 0
2. getsebol -a
3. audit2allow
4. semanage fcontext -a -t httpd_sys_content_t “/web(/.*)?” restorecon -R -v /web
5. /etc/sysconfig/selinux
6. По умолчанию в /var/log/audit/audit.log
7. getsebool -a | grep ftp
8. Просмотреть контекст безопасности процессора ps -eZ или id -Z

4 Выводы

Получены навыки работы с контекстом безопасности и политиками SELinux.