Лабораторная работа № 9

Отчёт

Ермишина Мария Кирилловна

Содержание

# 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. 1)

* sestatus -v Посмотрите, в каком режиме работает SELinux: (рис. 1)
* getenforce Измените режим работы SELinux на разрешающий (Permissive): (рис. 1)
* setenforce 0 и снова введите (рис. 1)
* getenforce

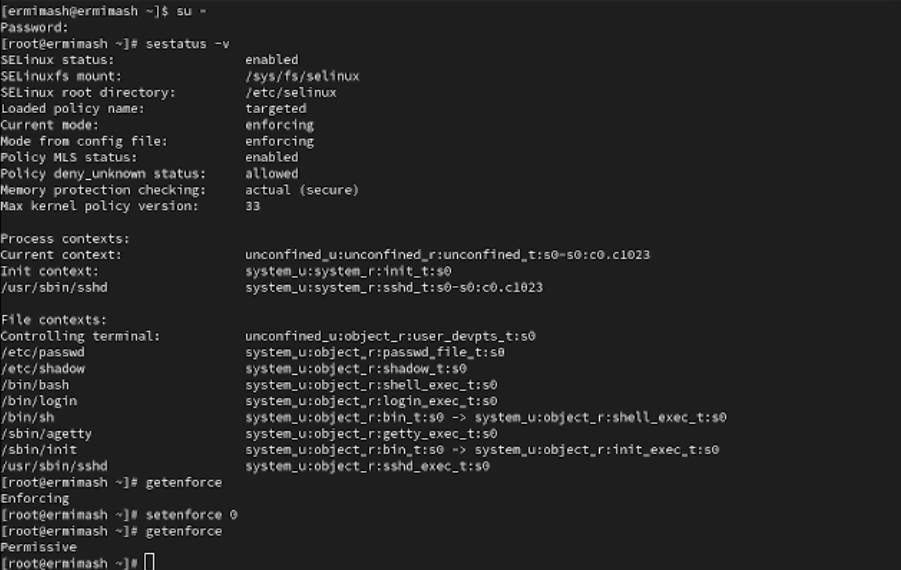


Рис. 1: Разрешающий режим SELinux

В файле /etc/sysconfig/selinux с помощью редактора установите: (рис. 2) - SELINUX=disabled

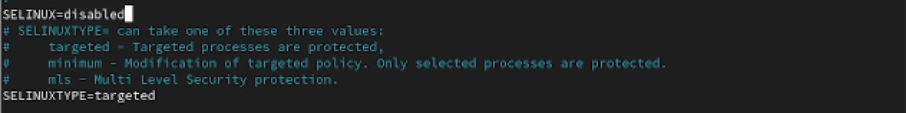


Рис. 2: disabled в файле SELinux

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

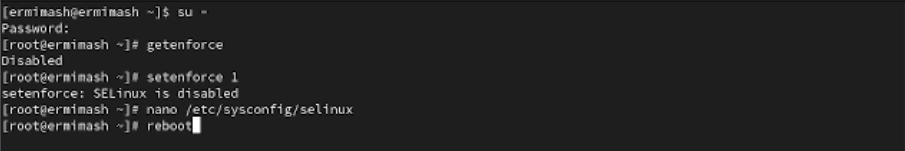


Рис. 3: Проверка изменений

Откройте файл /etc/sysconfig/selinux с помощью редактора и установите: (рис. 4) - SELINUX=enforcing Перезагрузите систему.

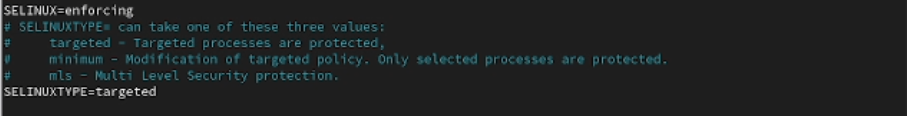


Рис. 4: enforcing в файле SELinux

После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux: (рис. 5) - sestatus -v

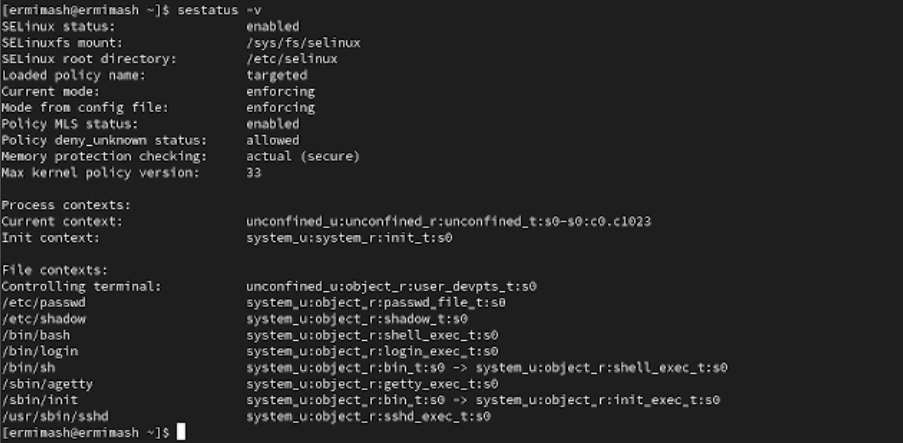


Рис. 5: Принудительный режим активен

1. Использование restorecon для восстановления контекста безопасности (рис. 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

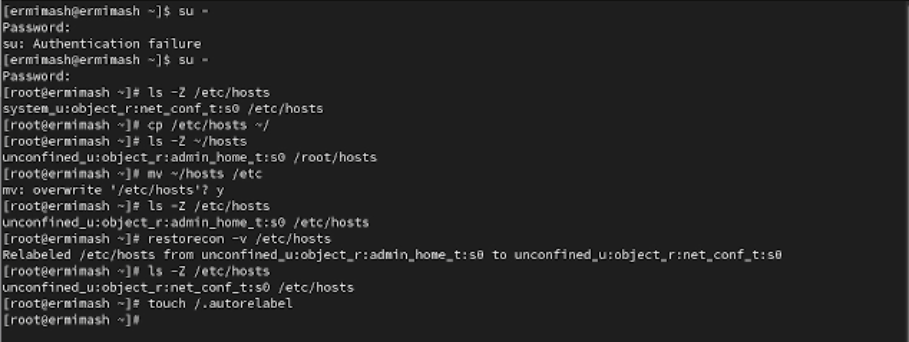


Рис. 6: Использование restorecon

1. Настройка контекста безопасности для нестандартного расположения файлов веб-сервера Запустите терминал и получите полномочия администратора. Установите необходимое программное обеспечение: (рис. 7)

* dnf -y install httpd
* dnf -y install lynx Создайте новое хранилище для файлов web-сервера: (рис. 7)
* mkdir /web Создайте файл index.html в каталоге с контентом веб-сервера: (рис. 7)
* cd /web
* touch index.html и поместите в файл следующий текст “Welcome to my web-server”

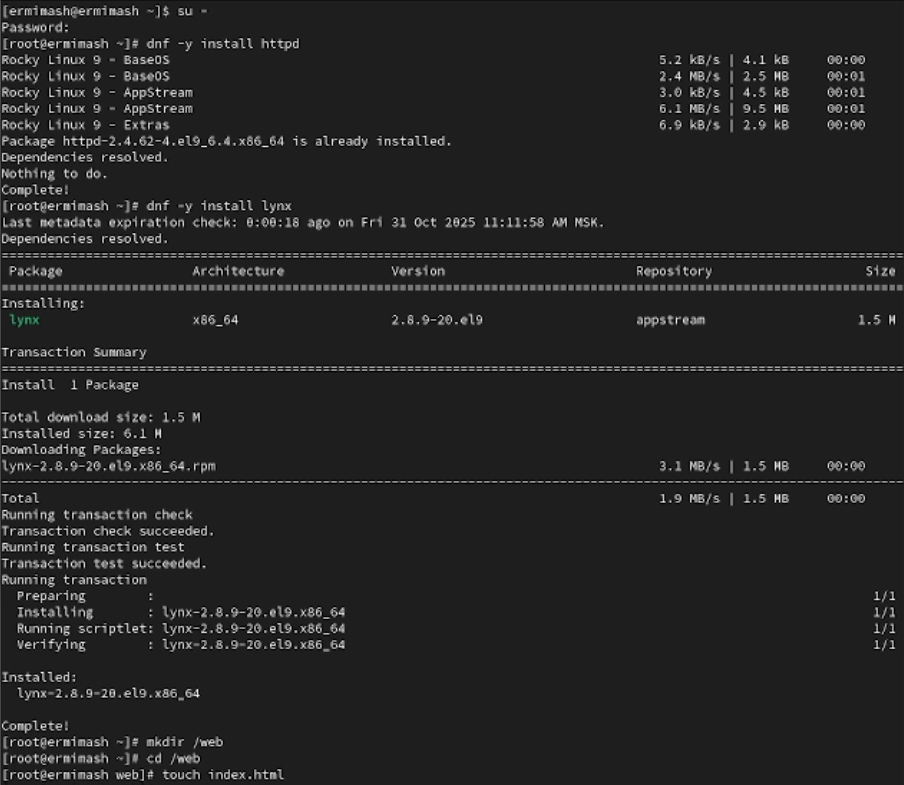


Рис. 7: Установка прог. обеспеч.

В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot “/var/www/html” и ниже добавьте строку “DocumentRoot”/web”” (рис. 8) Затем в этом же файле ниже закомментируйте раздел: (рис. 8) <Directory “/var/www”> AllowOverride None Require all granted и добавьте следующий раздел, определяющий правила доступа: (рис. 8) <Directory “/web”> AllowOverride None Require all granted

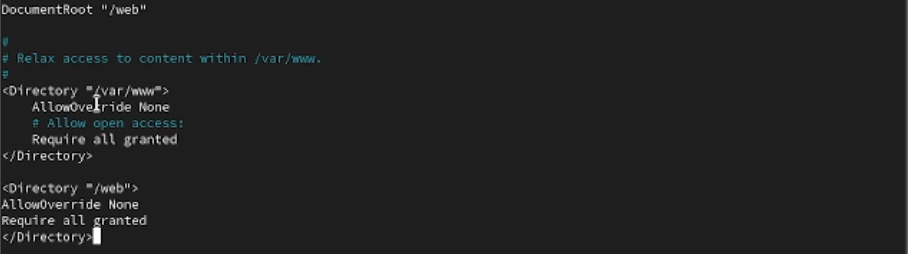


Рис. 8: Редакция текстового файла

Запустите веб-сервер и службу httpd: (рис. 10) - systemctl start httpd - systemctl enable httpd В терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx: (рис. 9) - lynx http://localhost

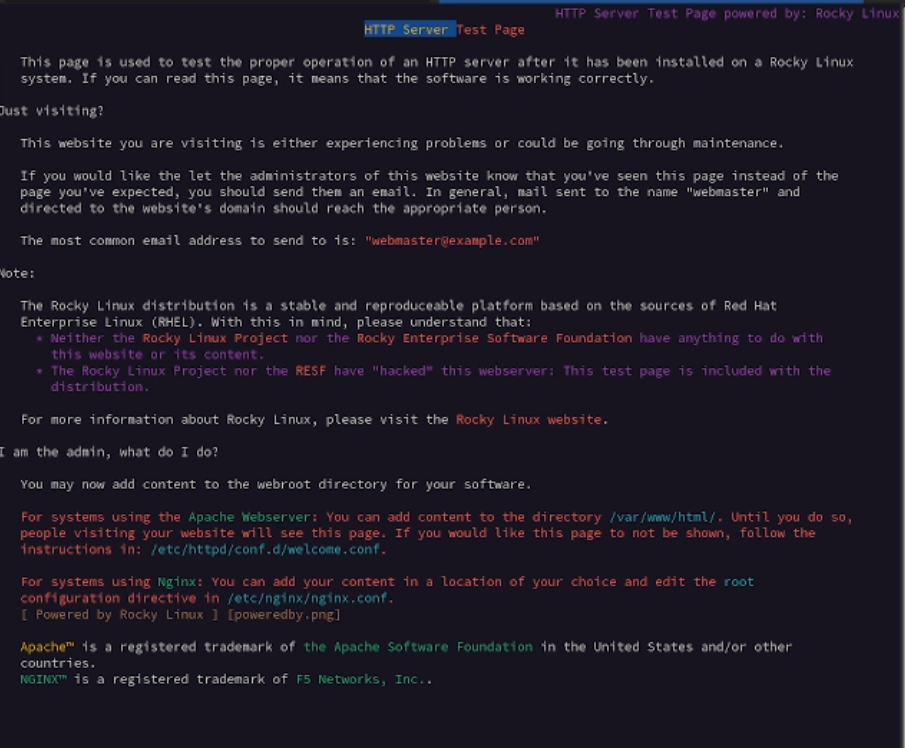


Рис. 9: Первый запуск сайта

В терминале с полномочиями администратора примените новую метку контекста к /web: (рис. 10) - semanage fcontext -a -t httpd\_sys\_content\_t “/web(/.\*)?” Восстановите контекст безопасности: (рис. 10) - restorecon -R -v /web



Рис. 10: Восстановка контекста безопасности

В терминале под учётной записью своего пользователя снова обратитесь к веб-серверу: (рис. 11) - lynx http://localhost

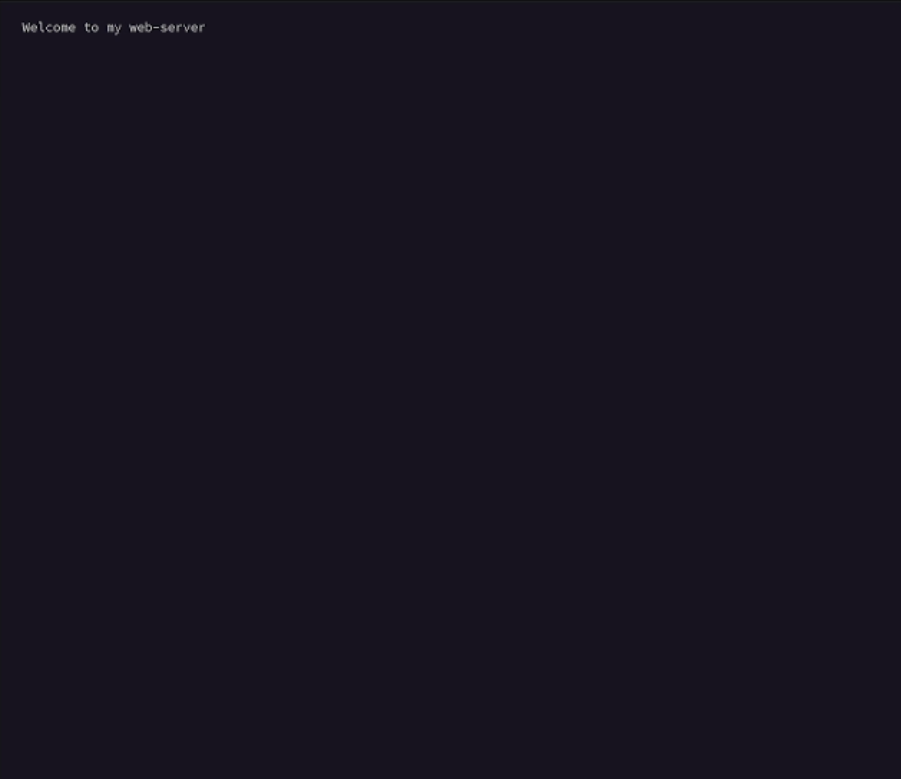


Рис. 11: Второй запуск

1. 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

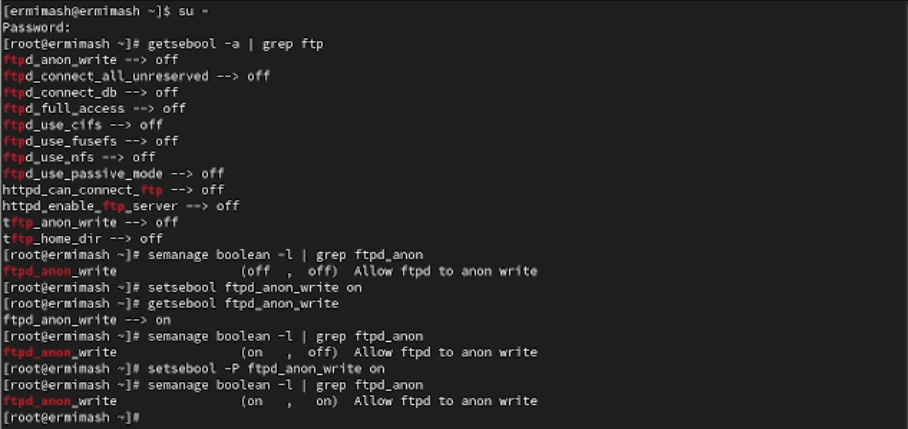


Рис. 12: Работа с переключателями SELinux

# 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.