Лабораторная работа №9

Управление SELinux

Ко Антон Геннадьевич

Содержание

Список иллюстраций

Список таблиц

# 1 РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

## 1.1 Факультет физико-математических и естественных наук

### 1.1.1 Кафедра прикладной информатики и теории вероятностей

# 2 ОТЧЕТ

## 2.1 ПО ЛАБОРАТОРНОЙ РАБОТЕ №9

### 2.1.1 дисциплина: Основы администрирования операционных систем

**Студент:** Ко Антон Геннадьевич  
**Студ. билет №:** 1132221551  
**Группа:** НПИбд-02-23

**МОСКВА**  
2024 г.

## 2.2 Цель работы:

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

## 2.3 Выполнение работы:

### 2.3.1 Управление режимами SELinux:

Запустим терминал и получим полномочия администратора:

su -

Просмотрим текущую информацию о состоянии SELinux:

sestatus -v

*Рис.1. Запуск терминала и получение полномочий администратора, просмотр текущей информации о состоянии SELinux.*

Посмотрим, в каком режиме работает SELinux:

getenforce

Изменим режим работы SELinux на разрешающий:

setenforce 0  
getenforce

Откроем файл /etc/sysconfig/selinux в текстовом редакторе:

mcedit /etc/sysconfig/selinux

*Рис. 2. Просмотр режима работы SELinux, изменение режима работы и проверка, открытие файла в текстовом редакторе.*

В открытом файле установим:

SELINUX=disabled

Сохраним изменения и перезагрузим систему:

reboot

*Рис.3. Установка в файле SELINUX=disabled, сохранение изменений и перезагрузка системы.*

После перезагрузки проверим статус SELinux:

getenforce

Попробуем переключить режим работы:

setenforce 1

Система сообщает, что SELinux отключён. Откроем файл /etc/sysconfig/selinux и установим:

SELINUX=enforcing

Сохраним изменения и перезагрузим систему.

### 2.3.2 Использование restorecon для восстановления контекста безопасности:

Просмотрим контекст безопасности файла /etc/hosts:

ls -Z /etc/hosts

Скопируем файл в домашний каталог и проверим контекст:

cp /etc/hosts ~/   
ls -Z ~/hosts

Переместим файл обратно в /etc и снова проверим контекст:

mv ~/hosts /etc/  
ls -Z /etc/hosts

Восстановим контекст безопасности:

restorecon -v /etc/hosts  
ls -Z /etc/hosts

Для массового исправления контекста выполним:

touch /.autorelabel  
reboot

*Рис. 10. Восстановление контекста безопасности.*

### 2.3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера:

Установим необходимое ПО:

dnf -y install httpd lynx

Создадим каталог и файл:

mkdir /web  
cd /web  
touch index.html

Откроем файл и добавим текст:

echo "Welcome to my web-server." > index.html

Изменим файл конфигурации Apache /etc/httpd/conf/httpd.conf, заменив DocumentRoot "/var/www/html" на DocumentRoot "/web". Также обновим настройки доступа.

Запустим веб-сервер:

systemctl start httpd  
systemctl enable httpd

Откроем веб-страницу в браузере:

lynx http://localhost

Применим новую метку контекста и восстановим контекст безопасности:

semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?"  
restorecon -R -v /web  
setenforce 1  
reboot

*Рис. 19. Настройка контекста безопасности для веб-сервера.*

### 2.3.4 Работа с переключателями SELinux:

Просмотрим список переключателей SELinux для службы ftp:

getsebool -a | grep ftp

Изменим значение переключателя:

setsebool ftpd\_anon\_write on  
getsebool ftpd\_anon\_write

Изменим постоянное значение переключателя:

setsebool -P ftpd\_anon\_write on  
semanage boolean -l | grep ftpd\_anon

*Рис. 25. Работа с переключателями SELinux.*

## 2.4 Ответы на контрольные вопросы:

1. setenforce 0
2. getsebool -a
3. audit2allow
4. bash semanage fcontext -a -t httpd\_sys\_content\_t "/web(/.\*)?" restorecon -R -v /web
5. /etc/sysconfig/selinux
6. /var/log/audit/audit.log
7. getsebool -a | grep ftp
8. ps -eZ или id -Z

## 2.5 Вывод:

В ходе выполнения лабораторной работы были получены навыки работы с контекстом безопасности и политиками SELinux.