

Отчёт по лабораторной работе №9.

Управление SELinux

Дисциплина: Основы администрирование операционных систем

Жукова Арина Александровна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Управление режимами SELinux	6
2.2	Использование restorecon для восстановления контекста безопасности	8
2.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	9
2.4	Работа с переключателями SELinux	12
3	Ответы на контрольные вопросы	14
4	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	Просмотр текущей информации	6
2.2	Просмотр режима, изменение режима	7
2.3	Изменение статуса с помощью редактора	7
2.4	Установка принудительного режима	8
2.5	Просмотр контекста безопасности файла, копирование файла, перезапись существующего файла	9
2.6	Исправление контекста безопасности, массовое исправление контекста	9
2.7	Установка программного обеспечения	10
2.8	Создание нового хранилища и файла	10
2.9	Изменение файла	10
2.10	Изменение файла	11
2.11	Запуск веб сервера и службы httpd	11
2.12	Обращение к веб-серверу	11
2.13	Применение новой метки к контексту, восстановление контекста .	12
2.14	Обращение к веб-серверу	12
2.15	Просмотр списка переключателей	13
2.16	Изменение текущего значения переключателя	13
2.17	Изменение постоянного значения переключателя	13

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).

```
[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# 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-c0.c1023
Init context:                  system_u:system_r:init_t:s0
/usr/sbin/sshd                 system_u:system_r:sshd_t: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:s0
/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
[root@aazhukoval ~]#
```

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).

```
[root@aazhukoval ~]# getenforce
Enforcing
[root@aazhukoval ~]# setenforce 0
[root@aazhukoval ~]# getenforce
Permissive
```

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).

```
[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# getenforce
Disabled
[root@aazhukoval ~]# setenforce 1
setenforce: SELinux is disabled
[root@aazhukoval ~]#
```

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).

```

[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# 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:s0
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
[root@aazhukoval ~]#

```

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).


```

[root@aazhukoval ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@aazhukoval ~]# cp /etc/hosts ~/
[root@aazhukoval ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@aazhukoval ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
[root@aazhukoval ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@aazhukoval ~]#

```

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).

```

[root@aazhukoval ~]# 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
[root@aazhukoval ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@aazhukoval ~]# touch /.autorelabel
[root@aazhukoval ~]#

```

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).

```
[root@aazhukoval ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                    5.7 kB/s | 4.1 kB      00:00
Rocky Linux 9 - BaseOS                    1.3 MB/s | 2.3 MB      00:01
Rocky Linux 9 - AppStream                  10 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream                  1.8 MB/s | 8.0 MB      00:04
Rocky Linux 9 - Extras                     6.3 kB/s | 2.9 kB      00:00
Пакет httpd-2.4.57-11.el9_4.1.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения.
Выполнено!
[root@aazhukoval ~]# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:02:07 назад, Чт 31 окт
2024 10:43:29.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий  Размер
=====
Установка:
lynx       x86_64      2.8.9-20.el9  appstream    1.5 М
```

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).

```
[root@aazhukoval ~]# mkdir /web
[root@aazhukoval ~]# cd /web
[root@aazhukoval web]# touch index.html
```

Рис. 2.8: Создание нового хранилища и файла

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

```
index.html  [-M--] 24 L: [ 1+ 0 1/ 1] *
Welcome to my web-server
```

Рис. 2.9: Изменение файла

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

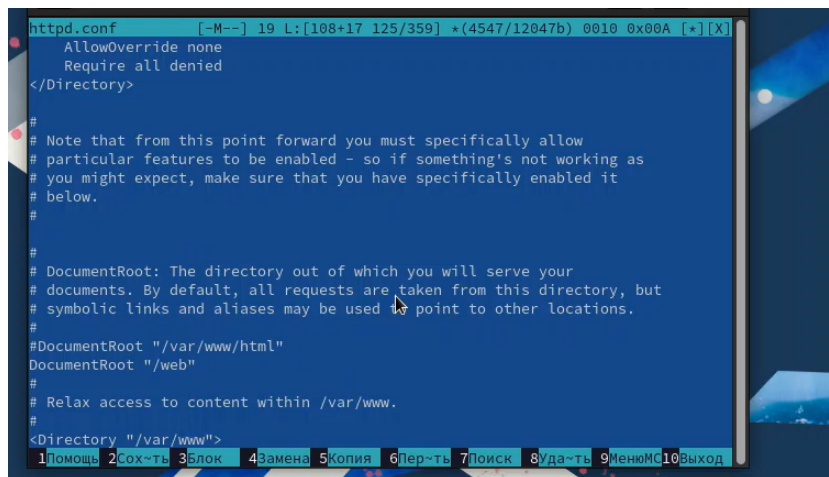


Рис. 2.10: Изменение файла

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

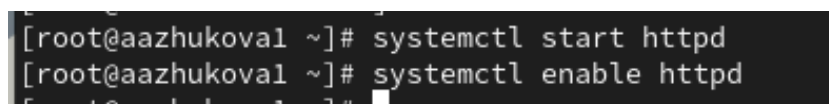


Рис. 2.11: Запуск веб сервера и службы httpd

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).

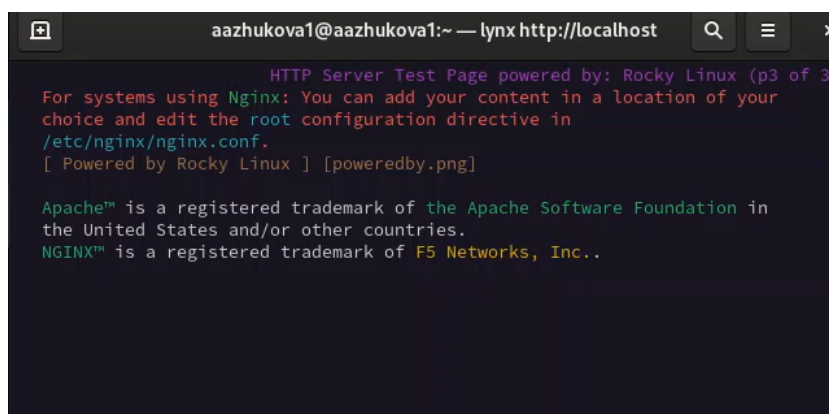


Рис. 2.12: Обращение к веб-серверу

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).

```
[root@aazhukoval ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@aazhukoval ~]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:
httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_
u:object_r:httpd_sys_content_t:s0
[root@aazhukoval ~]#
```

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).

```
Welcome to my web-server

Команды: стрелки - перемещение, '?' - помощь, 'q' - выход, '<-' - назад.
Стрелки: Вверх, Вниз - перемещение. Вправо - переход по ссылке; Влево - возвра
```

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).

```
[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# 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@aazhukoval ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
```

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).

```
[root@aazhukoval ~]# setsebool ftpd_anon_write on
[root@aazhukoval ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@aazhukoval ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
```

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).

```
[root@aazhukoval ~]# setsebool -P ftpd_anon_write on
[root@aazhukoval ~]#
[root@aazhukoval ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@aazhukoval ~]#
```

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 / М. 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.