Управление SELinux

Майоров Дмитрий Андреевич

Содержание i

1. Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2. Выполнение лабораторной работы

Получаем полномочия администратора. Смотрим текущую информацию о SELinux. SELinux включен(enabled) и находится в принудительном режиме работы (enforcing). Тип политики: targeted. Конфигурационный режим: enforcing. Состояние политики: MS status не задан, deny_unknown разрешен. Проверка защиты памяти активна. Версия ядра политики: 33

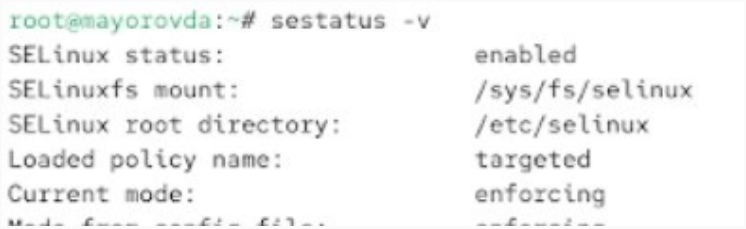


Рисунок 1

3. Выполнение лабораторной работы

Смотрим, в каком режиме работает SELinux.Он раюотает в принудительном режиме. Изменяем режим работы на разрешающий.

```
root@mayorovda:~# getenforce
Enforcing
root@mayorovda:~# setenforce 0
root@mayorovda:~# getenforce
Permissive
```

Рисунок 2

4. Выполнение лабораторной работы

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему

Рисунок 3

5. Выполнение лабораторной работы

Смотрим статус SELinux. Видим, что он отключен. Пробуем переключить режим работы. Система говорит, что SELInux отключен. Мы не можем переключаться между отключённым и принудительным режимом без перезагрузки системы

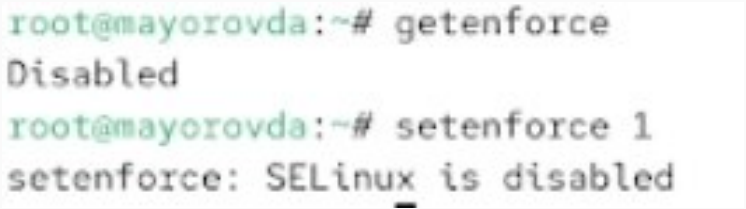


Рисунок 4

6. Выполнение лабораторной работы

Открываем файл /etc/sysconfig/selinux для редактирования и устанавливаем следующий параметр. Перезагружаем систему

Рисунок 5

7. Выполнение лабораторной работы

Смотрим текущую информацию о SELinux. Убеждаемся, что он работает в принудительном режиме

Рисунок 6

8. Выполнение лабораторной работы

Смотрм контекст безопасности файла /etc/hosts. Копируем его в домашний каталог. Проверяем контект файла. Параметр контекста изменился на admin_home_t

```
root@mayorovda:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@mayorovda:~# cp /etc/hosts ~/
root@mayorovda:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
```

Рисунок 7

Пытаемся перезаписать существующий файл hosts из домашнего каталога в каталог /etc. Убеждаемся, что тип контекста по-прежнему установлен на admin_home_t

```
root@mayorovda:~# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
root@mayorovda:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
```

Рисунок 8

10. Выполнение лабораторной работы

Исправляем контекст безопасности. Убеждаемся, что он изменился

```
root@mayorovda:~# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconf
ined_u:object_r:net_conf_t:s0
root@mayorovda:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
```

Рисунок 9

11. Выполнение лабораторной работы

Для массового исправления контекста безопасности на файловой системе вводим следующую команду и перезагружаем систему. При перезагрузке смотрим загрузочные сообщения. Видим, что файловая система перемаркирована

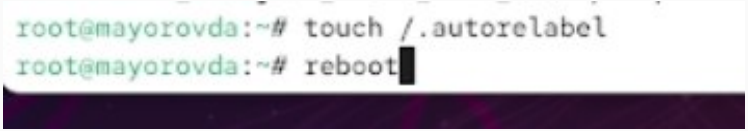
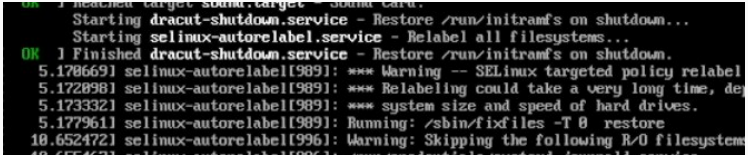


Рисунок 10



12. Выполнение лабораторной работы

Устанавливаем необходимое программное обеспечение

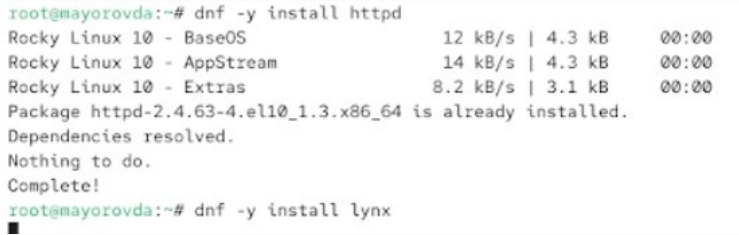


Рисунок 12

13. Выполнение лабораторной работы

Создаем новое хранилище для файлов web-сервера. Создаем файл index.html

```
root@mayorovda:~# mkdir /web
root@mayorovda:~# cd /web
root@mayorovda:/web# touch index.html
```

Рисунок 13

14. Выполнение лабораторной работы

Открываем этот файл для редактирования и помещаем туда следующий текст

Рисунок 14

15. Выполнение лабораторной работы

В файле /etc/httpd/conf/httpd.conf комментируем строку DocumentRoot «/var/www/html» и ниже добавляем строку DocumentRoot «/web»

Рисунок 15

Также ниже комментируем раздел и добавляем другой раздел, определяющий правила доступа

```
#<Directory "/var/www">
 #    AllowOverride None
     # Allow open access:
  #  Require all granted
#</Directory>

<Directory "/web">
     AllowOverride None
     Require all granted
```

17. Выполнение лабораторной работы

Запусткаем веб-сервер и службу httpd

```
root@mayorovda:/web# systemctl start httpd
root@mayorovda:/web# systemctl enable httpd
```

Рисунок 17

18. Выполнение лабораторной работы

Открваем веб-сервер в текстовом браузере. Видим страницу REd Hat по умолчанию

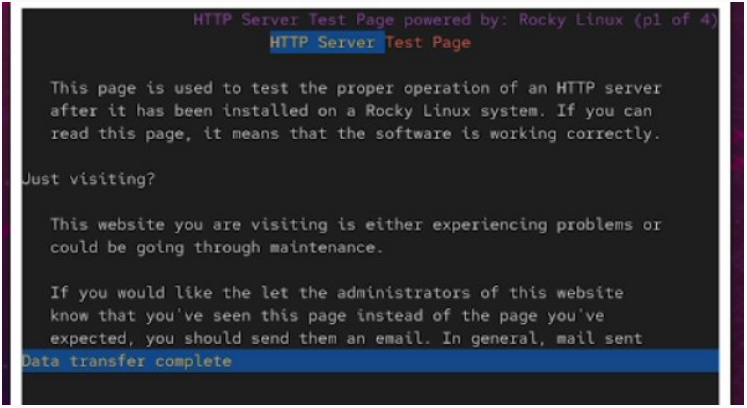


Рисунок 18

19. Выполнение лабораторной работы

Применяем новую метку контекста к /web и восстанавливаем контекст безопастности

```
root@mayorovda:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?
"
root@mayorovda:~# restorecon -R -v /web
```

Рисунок 19

20. Выполнение лабораторной работы

Перезагружаем систему и снова обращаемся к веб серверу. Теперь видим там запись, которую мы оставляли в файле index.html

Рисунок 20

21. Выполнение лабораторной работы

Смотрим список переключателей SELinux для службы ftp

```
mayorovda@mayorovda:~$ su -
Password:
Last login: Tue Feb  3 15:15:02 MSK 2026 on pts/0
root@mayorovda:~# 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
```

22. Выполнение лабораторной работы

Для службы ftpd_anon смотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен

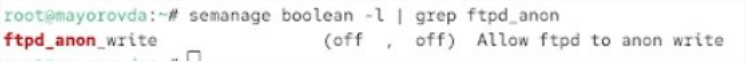


Рисунок 22

23. Выполнение лабораторной работы

Изменяем текущее значение переключателя для службы ftpd_anon_write с off на on. Снова смотрим список переключателей для службы ftpd_anon. Смотрим список всех переключатателей

```
root@mayorovda:~# setsebool ftpd_anon_write on
root@mayorovda:~# getsebool ftpd_anon_write
ftpd_anon_write --> on
root@mayorovda:~# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (on   ,  off)  Allow ftpd to anon write
```

Рисунок 23

24. Выполнение лабораторной работы

Изменяем постоянное значение переключателя для службы ftpd_anon_write с off на on. Смотрим список переключателей. Видим, что переключатель включен

25. Выводы

Получены навыки работы с контекстом безопасности и политиками SELinux.