

Управление SELinux

Майоров Дмитрий Андреевич

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

```
root@mayorovda:~# 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
```

Рисунок 1

3. Выполнение лабораторной работы

Смотрим, в каком режиме работает SELinux. Он работает 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

A screenshot of a text file, likely a terminal window or a text editor, showing the configuration of SELinux. The text is as follows:

SELINUX=disabled
SELINUXTYPE= can tal
The text is in a monospaced font, and the background is light gray. The first line is a comment starting with a hash symbol. The second line sets SELINUX to disabled. The third line is a comment starting with a hash symbol and followed by SELINUXTYPE= can tal.

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

```
root@mayorovda:~# getenforce
Disabled
root@mayorovda:~# setenforce 1
setenforce: SELinux is disabled
```

Рисунок 4

6. Выполнение лабораторной работы

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



```
#  
SELINUX=enforcing  
# SELINUXTYPE= can take
```

Рисунок 5

7. Выполнение лабораторной работы

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

```
root@mayorovda:~# 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
```

Рисунок 6

8. Выполнение лабораторной работы

Смотрим контекст безопасности файла /etc/hosts. Копируем его в домашний каталог. Проверяем контекст 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

9. Выполнение лабораторной работы

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

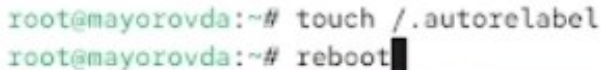
Исправляем контекст безопасности. Убеждаемся, что он изменился

```
root@mayorovda:~# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_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



```
root@mayorovda:~# touch /.autorelabel
root@mayorovda:~# reboot
```

Рисунок 10



```
OK 1 Reached target sound.target - Sound Card.
Starting dracut-shutdown.service - Restore /run/initramfs on shutdown...
Starting selinux-autorelabel.service - Relabel all filesystems...
OK 1 Finished dracut-shutdown.service - Restore /run/initramfs on shutdown.
5.178669] selinux-autorelabel[989]: *** Warning -- SELinux targeted policy relabel
5.172898] selinux-autorelabel[989]: *** Relabeling could take a very long time, dep
5.173332] selinux-autorelabel[989]: *** system size and speed of hard drives.
5.177961] selinux-autorelabel[989]: Running: /sbin/fixfiles -T 0 restore
18.652472] selinux-autorelabel[996]: Warning: Skipping the following R/O filesystems
48.655463] selinux-autorelabel[996]: *** Warning: SELinux targeted policy relabel
```

12. Выполнение лабораторной работы

Устанавливаем необходимое программное обеспечение

```
root@mayorovda:~# dnf -y install httpd
Rocky Linux 10 - BaseOS                12 kB/s | 4.3 kB      00:00
Rocky Linux 10 - AppStream              14 kB/s | 4.3 kB      00:00
Rocky Linux 10 - Extras                 8.2 kB/s | 3.1 kB      00:00
Package httpd-2.4.63-4.el10_1.3.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
root@mayorovda:~# dnf -y install lynx
█
```

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



```
GNU nano 8.1 index
Welcome to my web-server
```

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»`



```
#  
#DocumentRoot "/var/www/html"  
  
"
```

Рисунок 15

16. Выполнение лабораторной работы

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

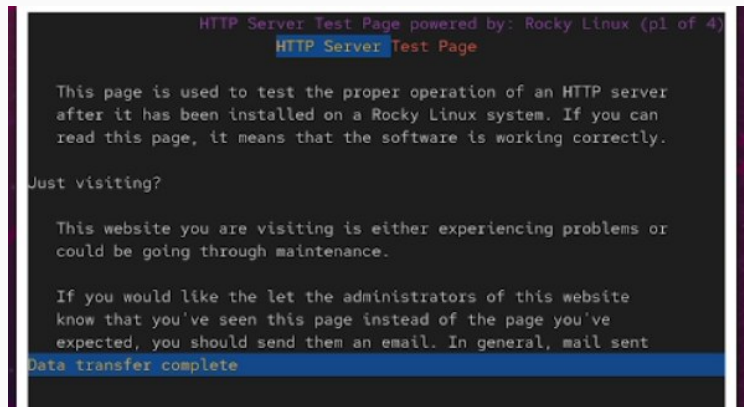
Запускаем веб-сервер и службу httpd

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

Рисунок 17

18. Выполнение лабораторной работы

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



```
HTTP Server Test Page powered by: Rocky Linux (pl of 4)
HTTP Server Test Page

This page is used to test the proper operation of an HTTP server
after it has been installed on a Rocky Linux system. If you can
read this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or
could be going through maintenance.

If you would like the let the administrators of this website
know that you've seen this page instead of the page you've
expected, you should send them an email. In general, mail sent
Data transfer complete
```

Рисунок 18

19. Выполнение лабораторной работы

Применяем новую метку контекста к /web и восстанавливаем контекст безопасности

```
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

A terminal window with a title bar containing a plus icon and the text 'mayorovda@mayorovda:~'. The terminal shows a command prompt 'mayorovda@mayorovda:~\$' followed by the command 'lynx http://localhost'.

```
mayorovda@mayorovda:~$ lynx http://localhost
```

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

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

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 переключателей

```
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.