Отчёт по лабораторной работе №6

Информационная безопасность

Арбатова Варвара Петровна

Содержание

Список таблиц

Список иллюстраций

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache. [@course]

2 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. SELinux имеет три основных режим работы:

Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [@f].

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA). Для чего нужен Apache сервер:

чтобы открывать динамические PHP-страницы,

для распределения поступающей на сервер нагрузки,

для обеспечения отказоустойчивости сервера,

чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

Более подробно см. в [@s].

3 Выполнение лабораторной работы

Перехожу в корневую директорию и устанавливаю httpd

```
[vparbatova@vparbatova ~]$ su root
Пароль:
[root@vparbatova vparbatova]# yum install httpd
packages for the GitHub CLI                    5.6 kB/s | 3.0 kB     00:00
packages for the GitHub CLI                    7.0 kB/s | 2.8 kB     00:00
Rocky Linux 9 - BaseOS                          12 kB/s | 4.1 kB     00:00
```

Рис. 3.1: Установка

Перехожу в директорию /etc/httpd, чтобы настроить веб-сервер. Добавляю строку ServerName test.ru в файл httpd.conf, указывая имя сервера. Очищаю правила iptables, чтобы сбросить настройки фаервола. Устанавливаю политику ACCEPT для входящих подключений, разрешая входящий трафик. Устанавливаю политику ACCEPT для исходящих подключений, разрешая исходящий трафик.

```
[root@vparbatova vparbatova]# cd /etc/httpd
[root@vparbatova httpd]# echo "ServerName test.ru" >> httpd.conf
[root@vparbatova httpd]# iptables -F
[root@vparbatova httpd]# iptables -P INPUT ACCEPT
[root@vparbatova httpd]# iptables -P OUTPUT ACCEPT
[root@vparbatova httpd]#
```

Рис. 3.2: Выполняю настройки

Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus

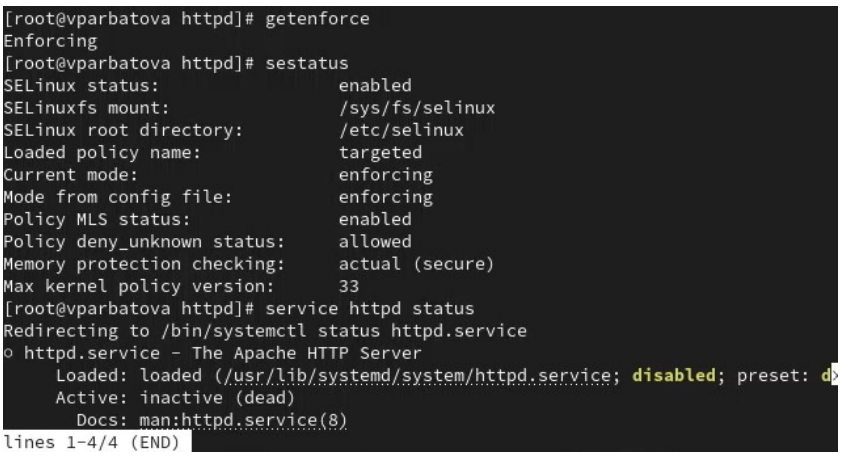

Рис. 3.3: Убеждаюсь в работе

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды service httpd status (рисунки 4-5)

Рис. 3.4: Запуск сервера

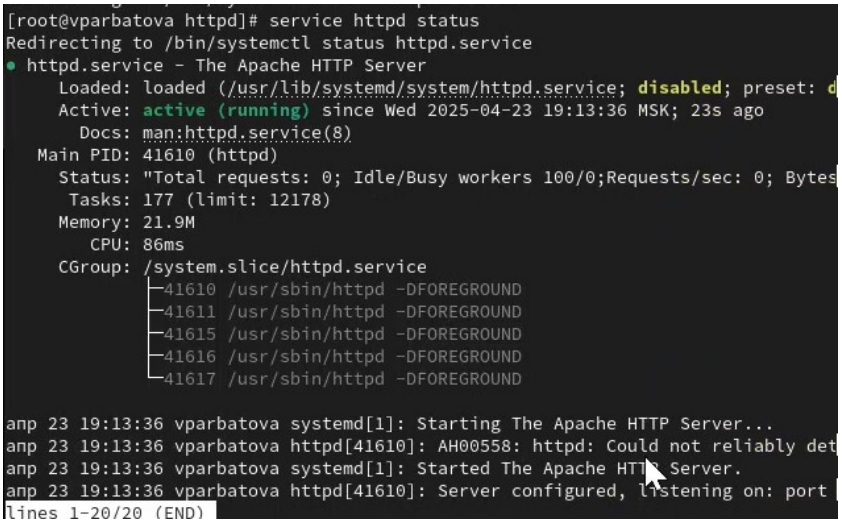

Рис. 3.5: Статус работы

С помощью команды ps auxZ | grep httpd нашла веб-сервер Apache в списке процессов. Его контекст безопасности - httpd_t

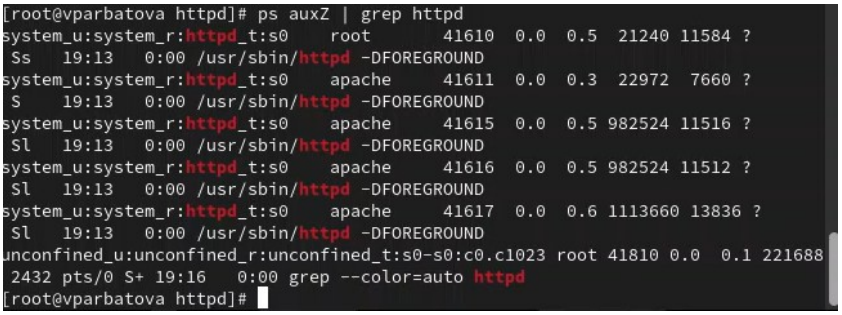

Рис. 3.6: Ищу контекст безопасности

Просмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd

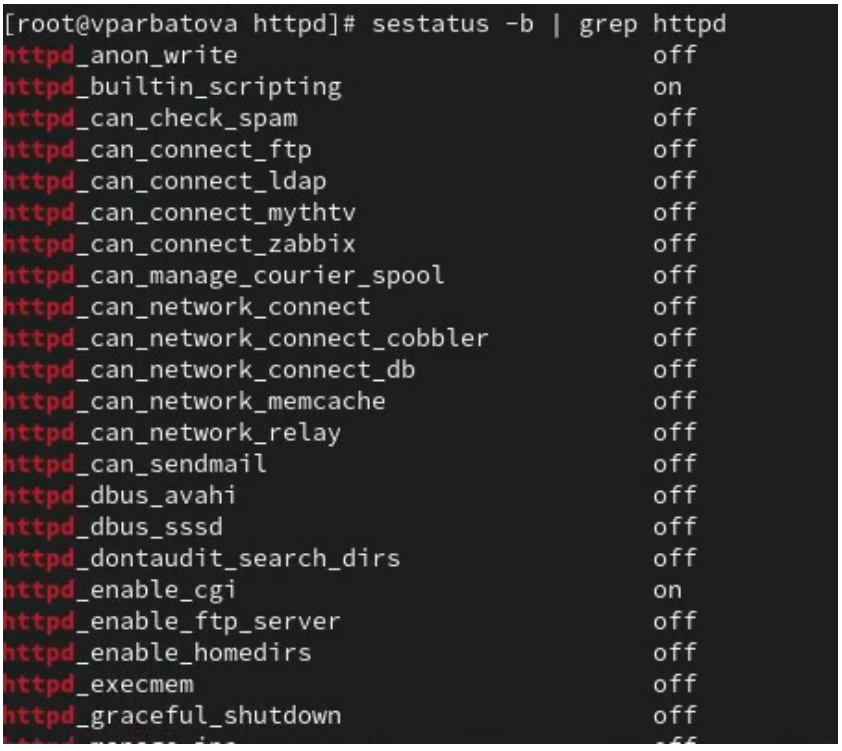

Рис. 3.7: Просмотр текущего состояния

Просмотрела статистику по политике с помощью команды seinfo. Множество

пользователей - 8, ролей - 39, типов - 5135

```
[root@vparbatova httpd]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5169    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            358    Cond. Expr.:         390
  Allow:             65633    Neverallow:            0
  Auditallow:          176    Dontaudit:          8703
  Type_trans:       271851    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           1    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               35
  Genfscon:            109    Portcon:             665
  Netifcon:              0    Nodecon:               0
[root@vparbatova httpd]#
```

Рис. 3.8: Просмотр статистики по политике

Типы поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www следующие: владелец - root, права на изменения только у владельца. Файлов в директории нет

```
[root@vparbatova httpd]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 янв 22 03:
25 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 янв 22 03:
25 html
[root@vparbatova httpd]#
```

Рис. 3.9: Смотрю права

В директории /var/www/html нет файлов.

Рис. 3.10: Файлы директории

Создаю файл

Рис. 3.11: Создание файла

Создать файл может только суперпользователь, поэтому от его имени создаем файл touch.html со следующим содержанием

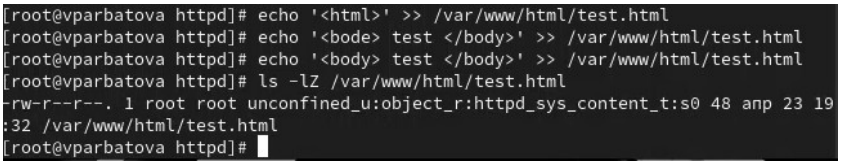

Рис. 3.12: Заполняю файл

Перехожу на сайт и смотрю. Всё удачно

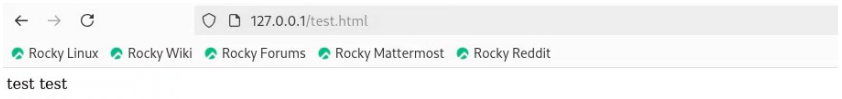

Рис. 3.13: Сайт

Изменяю контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html Контекст действительно поменялся

```
[root@vparbatova httpd]# chcon -t samba_share_t /var/www/html/test.html
[root@vparbatova httpd]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 48 апр 23 19:32 /v
ar/www/html/test.html
[root@vparbatova httpd]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vparbatova httpd]#
```

Рис. 3.14: Изменение контекста

Доступ запрещен

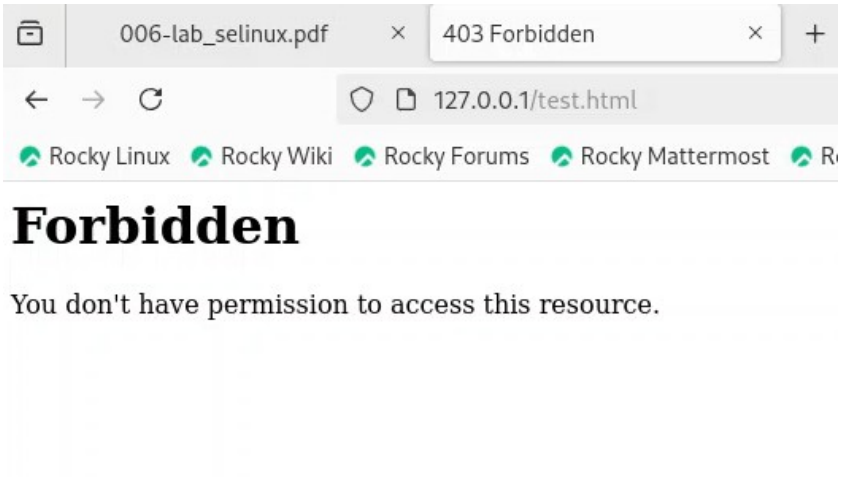

Рис. 3.15: Сайт

файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю, потому что установлен контекст, к которому процесс httpd не должен иметь доступа.

Просматриваю log-файлы веб-сервера Apache и системный лог-файл: tail /var/log/messages. Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log

```
[root@vparbatova httpd]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 48 апр 23 19:32 /var/www/html/test.html
[root@vparbatova httpd]# tail /var/log/messages
Apr 23 19:38:56 vparbatova setroubleshoot[42764]: SELinux запрещает /usr/sbin/htt
pd доступ getattr к файл /var/www/html/test.html.#012#012*****  Модуль restorecon
 предлагает (точность 92.2)  **************************#012#012Если вы хотите испр
авить метку.$TARGET3нак _PATH по умолчанию должен быть httpd_sys_content_t#012To
вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за
недостаточных разрешений для доступа к родительскому каталогу, и в этом случае по
пытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sb
in/restorecon -v /var/www/html/test.html#012#012*****  Модуль public_content пред
лагает (точность 7.83)  **********************#012#012Если вы хотите лечить test.h
tml как общедоступный контент#012To необходимо изменить метку test.html с public_
```

Рис. 3.16: Проверка

4 Выводы

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы