

Отчёт по лабораторной работе №6

Простейший шаблон

Абрамян А. А.

2023, 30 сентября Москва, Россия

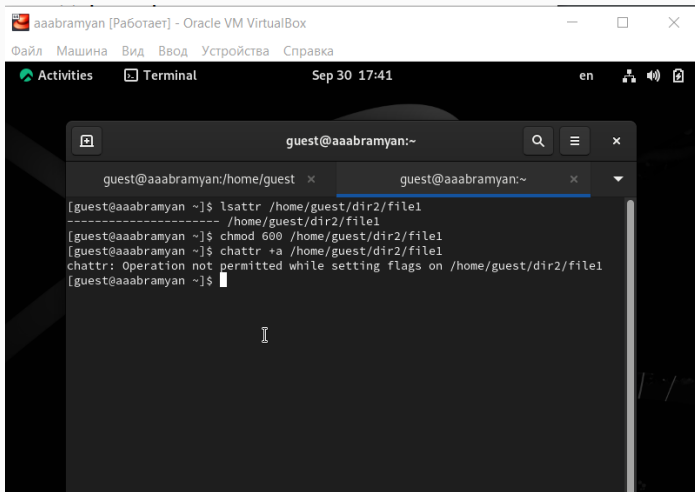
Российский университет дружбы народов, Москва, Россия

- решить поставленную задачу;
- решить возникающие трудности и проблемы;
- практически получить полезный результат;

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

1. Вошёл в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus” (рис. 1)



The screenshot shows a terminal window titled "aaabramyan [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a toolbar with "Activities", "Terminal", and a clock showing "Sep 30 17:41". The terminal itself has a title bar "guest@aaabramyan:~" and a search icon. It contains two tabs: "guest@aaabramyan:/home/guest" and "guest@aaabramyan:~". The terminal output shows the following commands and results:

```
[guest@aaabramyan ~]$ lsattr /home/guest/dir2/file1
----- /home/guest/dir2/file1
[guest@aaabramyan ~]$ chmod 600 /home/guest/dir2/file1
[guest@aaabramyan ~]$ chattr +a /home/guest/dir2/file1
chattr: Operation not permitted while setting flags on /home/guest/dir2/file1
[guest@aaabramyan ~]$
```

2. Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере, убедился, что последний работает с помощью команды “service httpd status” (рис. 2)

Проверка работы веб-сервера

Рис. 2: Проверка работы веб-сервера

3. С помощью команды `"ps auxZ | grep httpd"` определил контекст безопасности веб-сервера Apache - `httpd_t` (рис. 3)

Контекст безопасности веб-сервера Apache

Рис. 3: Контекст безопасности веб-сервера Apache

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `"sestatus -bigrep httpd"`, многие из переключателей находятся в положении "off" (рис. 4)

Текущее состояние переключателей SELinux

Рис. 4: Текущее состояние переключателей SELinux

5. С помощью команды `ls -lZ /var/www` посмотрел файлы и поддиректории, находящиеся в директории `/var/www`. Используя команду `ls -lZ /var/www/html`, определил, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории `/var/www/html` (рис. ??)

Просмотр файлов и поддиректорий в директории `/var/www`

Рис. 5: Просмотр файлов и поддиректорий в директории `/var/www`

6. Обратился к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен. Изучив справку `man httpd_selinux`, выяснил, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`. Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменил контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверил, что контекст поменялся (рис. 11)

Запуск программы `readfile`

Рис. 6: Запуск программы `readfile`

7. Командой `ls -l /var/www/html/test.html` убедился, что читать данный файл может любой пользователь. Просмотрел системный лог-файл веб-сервера Apache командой `sudo tail /var/log/messages`, отображающий ошибки (рис. ??)

Просмотр log-файла

Рис. 7: Просмотр log-файла

8. От имени пользователя guest2 попробовал прочитать файл командой `"cat /tmp/file01.txt"` - это удалось. Далее попытался дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой `"chmod g+rw /tmp/file01.txt"`. От имени пользователя guest2 попробовал удалить файл - это не удастся ни в каком из случаев, возникает ошибка (рис. ??)

Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

Рис. 8: Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

9. Повысил права до суперпользователя командой `"su -"` и выполнил команду, снимающую атрибут t с директории /tmp `"chmod -t /tmp"`. После чего покинул режим суперпользователя командой `"exit"`. Повторил предыдущие шаги. Теперь мне удалось

10. Удалил файл `"/var/www/html/test.html"` командой `"rm /var/www/html/test.html" /tmp` (рис. ??)

Удаление файла test.html

Рис. 10: Удаление файла test.html

10. Повысил права до суперпользователя командой “su -” и выполнил команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинул режим суперпользователя командой “exit”. Повторил предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp (рис. ??)

Возвращение атрибута t (Sticky-бита)

Рис. 11: Возвращение атрибута t (Sticky-бита)

- В данной лабораторной работе мне успешно удалось Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.