Лабораторная работа №6

Информационная безопасность

Аристова А. О.

11 октября 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Докладчик

- Аристова Арина Олеговна
- Студентка группы НФИбд-01-21
- Студ. билет 1032216433
- Российский университет дружбы народов имени Патриса Лумумбы

Цель лабораторной работы

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

Теоретическая справка (1)

1. **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

Теоретическая справка (1)

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.

Теоретическая справка (2)

2. **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)

Теоретическая справка (2)

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.

Ход выполнения лабораторной работы

Выполнение лабораторной работы

Убедились, что SELinux работает в режиме enforcing политики targeted

```
[mvmalashenko@mvmalashenko ~]$ cat /etc/httpd/httpd.conf
cat: /etc/httpd/httpd.conf: No such file or directory
[mvmalashenko@mvmalashenko ~]$ getenforce
Enforcing
[mvmalashenko@mvmalashenko ~]$ sestatus
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
```

Рис. 1: (рис. 1. Проверка режима enforcing политики targeted)

Выполнение лабораторной работы

Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает

(рис. 2. Проверка работы веб-сервера)

Рис. 2: (рис. 2. Проверка работы веб-сервера)

Выполнение лабораторной работы

Определили контекст безопасности веб-сервера Apache

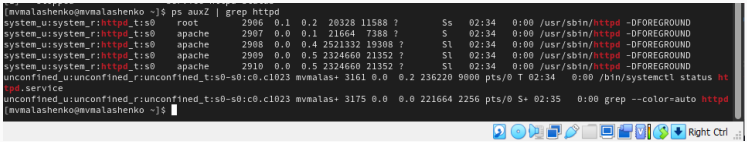


Рис. 3: (рис. 3. Контекст безопасности веб-сервера Apache)

Выполнение лабораторной работы

Посмотрели текущее состояние переключателей, многие из переключателей находятся в положении “off”

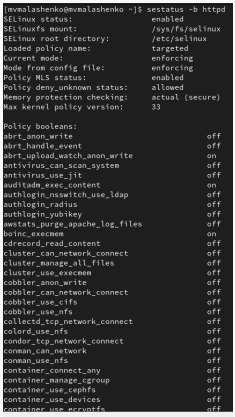


Рис. 4: (рис. 4. Текущее состояние переключателей SELinux)

Выполнение лабораторной работы

Посмотрели статистику по политике. Множество пользователей - 8, ролей - 14, типов 5100

```
 * Waiting in queue...
 * Waiting for authentication...
 * Waiting in queue...
 * Downloading packages...
 * Requesting data...
 * Testing changes...
 * Installing packages...
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:              5100    Attributes:          258
  Users:                 8    Roles:                14
  Booleans:            353    Cond. Expr.:         384
  Allow:             65000    Neverallow:            0
  Auditallow:          170    Dontaudit:          8572
  Type_trans:       265341    Type_change:          87
  Type_member:          35    Range_trans:        6164
  Role allow:           38    Role_trans:          420
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           2    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:             660
  Netifcon:              0    Nodecon:               0
```


Рис. 5: (рис. 5. Статистика по политике)

Выполнение лабораторной работы

Посмотрели файлы и поддиректории, находящиеся в директории /var/www. Определили, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html

Рис. 6: (рис. 6. Просмотр файлов и поддиректориий в директории /var/www)

Выполнение лабораторной работы

От имени суперпользователя создали html-файл. Контекст созданного файла - httpd_sys_content_t

```
[mvmalashenko@mvmalashenko ~]$ su -
Password:
[root@mvmalashenko ~]# touch /var/www/html/test.html
[root@mvmalashenko ~]# nano /var/www/html/test.html
[root@mvmalashenko ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@mvmalashenko ~]# su - mvmalashenko
[mvmalashenko@mvmalashenko ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 13 02:43 test.html
```

Рис. 7: (рис. 7. Создание файла /var/www/html/test.html)

Выполнение лабораторной работы

Обратились к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен

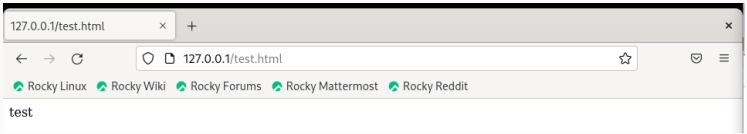


Рис. 8: (рис. 8. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Изучив справку httpd_selinux, выяснили, какие контексты определены для файлов httpd.

Контекст моего файла - httpd_sys_content_t (в таком случае содержимое должно быть доступно для всех скриптов httpd и для самого демона). Изменили контекст файла на samba_share_t

```
[mvmalashenko@mvmalashenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to ‘unconfined_u:
object_r:samba_share_t:s0’: Operation not permitted
[mvmalashenko@mvmalashenko ~]$ sudo chcon -t samba_share_t /var/www/html/test.
html
[sudo] password for mvmalashenko:
[mvmalashenko@mvmalashenko ~]$ chcon -t samba_share_t /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 9: (рис. 9. Изменение контекста)

Выполнение лабораторной работы

Попробовали еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получили сообщение об ошибке (т.к. кустановленному ранее контексту процесс httpd не имеет доступа)

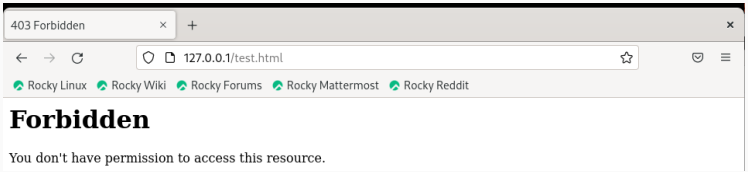
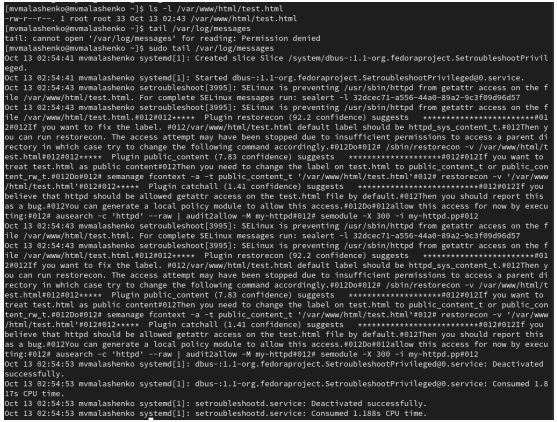


Рис. 10: (рис. 10. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Убедились, что читать данный файл может любой пользователь.
Просмотрели системный лог-файл веб-сервера Apache, отображающий ошибки



Выполнение лабораторной работы

В файле /etc/httpd/conf/httpd.conf заменили строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81

Рис. 12: (рис. 12. Установка веб-сервера Apache на прослушивание TCP-порта 81)

Выполнение лабораторной работы

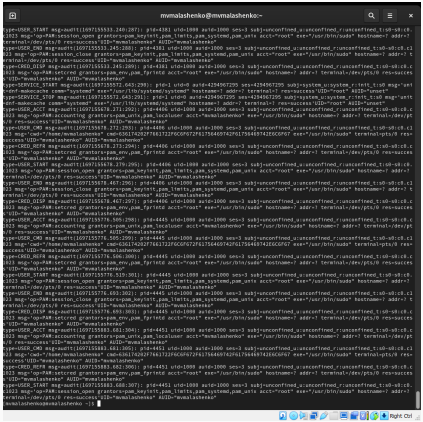
Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -nl /var/log/messages”

```
[mvmalashenko@mvmalashenko ~]$ systemctl restart httpd
[mvmalashenko@mvmalashenko ~]$ tail -nl /var/log/messages
tail: invalid number of lines: ‘l’
[mvmalashenko@mvmalashenko ~]$ tail -n1 /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[mvmalashenko@mvmalashenko ~]$ sudo tail -n1 /var/log/messages
Oct 13 03:03:22 mvmalashenko systemd[1]: fprintd.service: Deactivated successfully.
```

Рис. 13: (рис. 13. Перезапуск веб-сервера и анализ лог-файлов)

Выполнение лабораторной работы

Просмотрели файлы “var/log/http/error_log”, “/var/log/http/access_log” и “/var/log/audit/audit.log” и выяснили, что запись появилась в последнем файле



Выполнение лабораторной работы

Проверили список портов командой, убедились, что порт 81 есть в списке и запускаем веб-сервер Apache снова

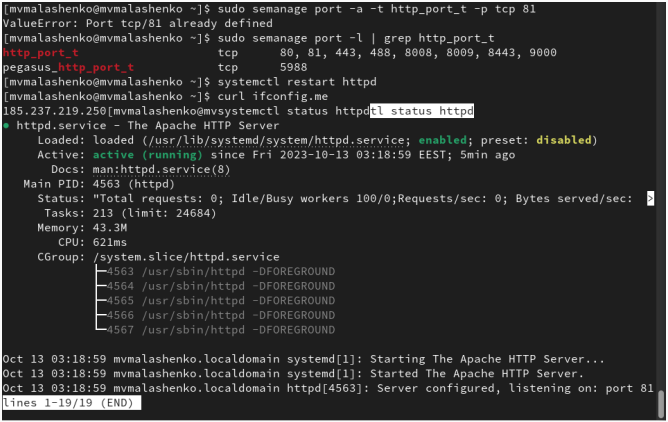


Рис. 15: (рис. 15. Проверка установки порта 81)

Выполнение лабораторной работы

Вернули контекст “httpd_sys_content_t” файлу “/var/www/html/test.html” и попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, увидели содежимое файла - слово “test”

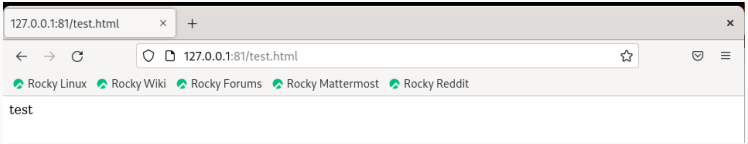


Рис. 16: (рис. 17. Обращение к файлу через веб-сервер)

Выполнение лабораторной работы

Исправили обратно конфигурационный файл apache, вернув “Listen 80”. Попытались удалить привязку http_port к 81 порту, но этот порт определен на уровне политики, поэтому его нельзя удалить

Выполнение лабораторной работы

Удалили файл “/var/www/html/test.html”

```
[mvmalashenko@mvmalashenko ~]$ sudo rm /var/www/html/test.html
[mvmalashenko@mvmalashenko ~]$ ls /var/www/html/test.html
ls: cannot access '/var/www/html/test.html': No such file or directory
[mvmalashenko@mvmalashenko ~]$ ls /var/www/html
```

Рис. 18: (рис. 19. Удаление файла test.html)

Вывод

Вывод

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. Библиография

Список литературы. Библиография

0] Методические материалы курса

[1] SELinux: https://habr.com/ru/companies/kingservers/articles/209644/

[2] Apache: https://2domains.ru/support/vps-i-servery/shto-takoye-apache