

Защита лабораторной работы №6

Информационная безопасность

Шатохина В. С.

2024

Российский университет дружбы народов, Москва, Россия

- Шатохина Виктория Сергеевна
- Студентка группы НФИбд-02-21
- Студ. билет 1032217046
- Российский университет дружбы народов

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

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

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.

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)

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

```
Complete!  
[mmalashenko@mmalashenko ~]$ sudo systemctl start httpd  
[mmalashenko@mmalashenko ~]$ sudo systemctl enable httpd  
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.  
[mmalashenko@mmalashenko ~]$ service httpd status  
Redirecting to /bin/systemctl status httpd.service  
* httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: 1  
   Active: active (running) since Fri 2023-10-13 02:34:11 EEST; 19s ago  
     Docs: man:httpd.service(8)  
  Main PID: 2906 (httpd)  
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes  
   Tasks: 213 (limit 24004)  
  Memory: 40.7M  
    CPU(s): 266ms  
  CGroup: /system.slice/httpd.service  
          └─2906 /usr/sbin/httpd -DFOREGROUND  
            └─2907 /usr/sbin/httpd -DFOREGROUND  
              └─2908 /usr/sbin/httpd -DFOREGROUND  
                └─2909 /usr/sbin/httpd -DFOREGROUND  
                  └─2910 /usr/sbin/httpd -DFOREGROUND  
  
Oct 13 02:34:10 mmalashenko.localdomain systemd[1]: Starting The Apache HTTP  
Oct 13 02:34:11 mmalashenko.localdomain systemd[1]: Started The Apache HTTP  
Oct 13 02:34:11 mmalashenko.localdomain httpd[2906]: Server configured, 1 stat  
lines 1-19/19 (END)
```

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

Определили контекст безопасности веб-сервера Apache



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

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: 198 Permissions: 497
Sensitivities: 1 Categories: 1824
Types: 5100 Attributes: 258
Users: 8 Roles: 14
Booleans: 353 Cond. Expr.: 384
Allow: 61608 Generalized: 8
Auditallow: 119 Dostaudit: 6672
Type_trans: 265341 Type_change: 87
Type_member: 20 Range_trans: 6164
Role_allow: 20 Role_trans: 428
Constraints: 70 Validatetrans: 8
MLS Constraints: 72 MLS Val. Trans: 8
Permissions: 2 Policy: 8
Defaults: 7 Typebounds: 8
Allowperms: 8 Neverallowperms: 8
Auditallowperms: 8 Dostauditperms: 8
Ibendportcon: 8 Ibskeycon: 8
Initial SIDs: 27 Paused: 23
Genfscon: 188 Portcon: 688
Netifcon: 8 Nodecon: 8
```

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

```
[evmalashenko@evmalashenko ~]$ ls -lZ /var/www
total 8
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 13:21 html
[evmalashenko@evmalashenko ~]$ ls -lZ /var/www/html
total 8
```

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

Выполнение лабораторной работы

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

```
[mmalashenko@mmalashenko ~]$ su -  
Password:  
[root@mmalashenko ~]# touch /var/www/html/test.html  
[root@mmalashenko ~]# nano /var/www/html/test.html  
[root@mmalashenko ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@mmalashenko ~]# su - mmalashenko  
[mmalashenko@mmalashenko ~]# 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



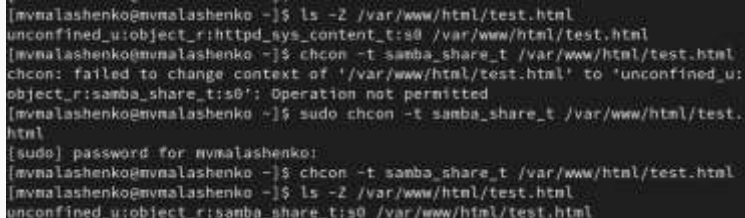
Рис. 8: (рис. 8. Обращение к файлу через веб-сервер)

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

[illegible]

Рис. 11: (рис. 11. Просмотр log-файла)

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)

Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -n1 /var/log/messages”

```
[evmalashenko@evmalashenko ~]$ systemctl restart httpd
[evmalashenko@evmalashenko ~]$ tail -n1 /var/log/messages
tail: invalid number of lines: '1'
[evmalashenko@evmalashenko ~]$ tail -n1 /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[evmalashenko@evmalashenko ~]$ sudo tail -n1 /var/log/messages
Oct 13 03:03:22 evmalashenko 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



Рис. 14: (рис. 14. Содержание файла var/log/audit/audit.log)

Выполнение лабораторной работы

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

```
[wwwalashenko@wwwalashenko ~]$ sudo semanage port -a -t http_port_t -p tcp 81
valueError: Port tcp/81 already defined
[wwwalashenko@wwwalashenko ~]$ sudo semanage port -l | grep http_port_t
tcp_port_t          tcp      80, 81, 443, 488, 8080, 8089, 9443, 9908
pegasus_http_port_t tcp      5050
[wwwalashenko@wwwalashenko ~]$ systemctl restart httpd
[wwwalashenko@wwwalashenko ~]$ curl ifconfig.me
185.237.239.250[wwwalashenko@wwwalashenko ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2023-10-13 03:18:39 EEST; 3min ago
     Docs: man:httpd.service(8)
   Main PID: 4563 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; requests/sec: 0; Bytes served/sec: 0"
     Tasks: 111 (limit: 24584)
  Memory: 43.3M
     CPU: 621ms
   CGroup: /system.slice/httpd.service
           └─4563 /usr/sbin/httpd -DFOREGROUND
             └─4564 /usr/sbin/httpd -DFOREGROUND
               └─4565 /usr/sbin/httpd -DFOREGROUND
                 └─4566 /usr/sbin/httpd -DFOREGROUND
                   └─4567 /usr/sbin/httpd -DFOREGROUND

Oct 13 03:18:39 wwwalashenko.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 13 03:18:50 wwwalashenko.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 13 03:18:59 wwwalashenko.localdomain httpd[4563]: Server configured, listening on: port 81
Times: 1-19/10 (PMO)
```

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 содержимое 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

[illegible]

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

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

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>