

Отчёт по лабораторной работе №6

Информационная безопасность

Мандатное разграничение прав в Linux

Выполнила: Сингх Ааруши ,
НКАбд-02-23, 132215095

Содержание

Цель работы	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Вывод.....	8
Список литературы. Библиография	8

Цель работы

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

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 [1].

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:

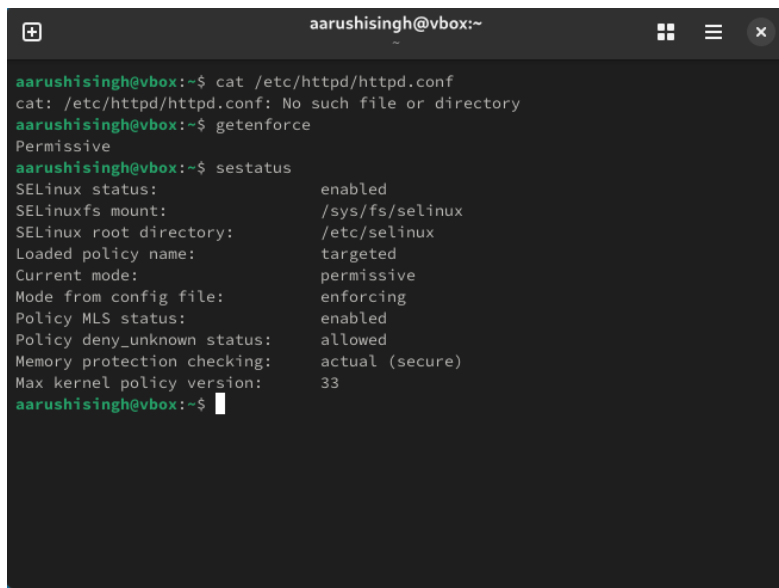
- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

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

Более подробно см. в [2].

Выполнение лабораторной работы

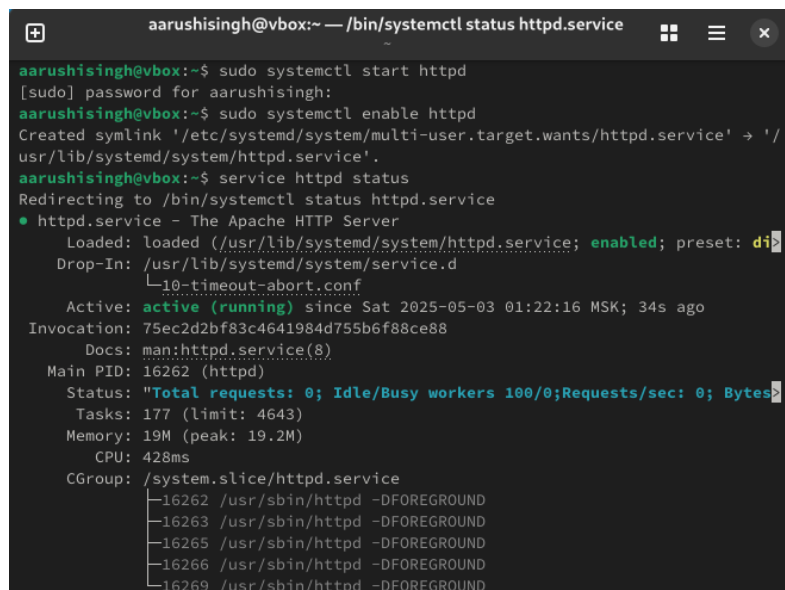
Вошли в систему под своей учетной записью и убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”



```
aarushisingh@vbox:~  
aarushisingh@vbox:~$ cat /etc/httpd/httpd.conf  
cat: /etc/httpd/httpd.conf: No such file or directory  
aarushisingh@vbox:~$ getenforce  
Permissive  
aarushisingh@vbox:~$ sestatus  
SELinux status:                enabled  
SELinuxfs mount:                /sys/fs/selinux  
SELinux root directory:         /etc/selinux  
Loaded policy name:              targeted  
Current mode:                    permissive  
Mode from config file:           enforcing  
Policy MLS status:               enabled  
Policy deny_unknown status:      allowed  
Memory protection checking:      actual (secure)  
Max kernel policy version:       33  
aarushisingh@vbox:~$
```

(рис. 1. Проверка режима enforcing политики targeted)

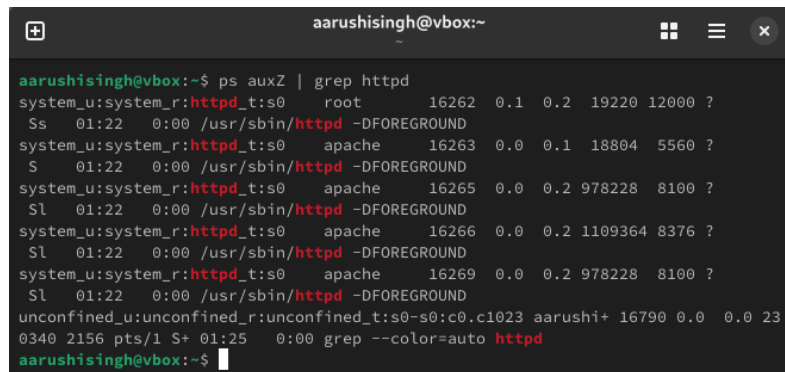
Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает с помощью команды “service httpd status”



```
aarushisingh@vbox:~ — /bin/systemctl status httpd.service
aarushisingh@vbox:~$ sudo systemctl start httpd
[sudo] password for aarushisingh:
aarushisingh@vbox:~$ sudo systemctl enable httpd
Created symlink '/etc/systemd/system/multi-user.target.wants/httpd.service' → '/usr/lib/systemd/system/httpd.service'.
aarushisingh@vbox:~$ 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: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Sat 2025-05-03 01:22:16 MSK; 34s ago
   Invocation: 75ec2d2bf83c4641984d755b6f88ce88
   Docs: man:httpd.service(8)
   Main PID: 16262 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes"
   Tasks: 177 (limit: 4643)
   Memory: 19M (peak: 19.2M)
   CPU: 428ms
   CGroup: /system.slice/httpd.service
           └─16262 /usr/sbin/httpd -DFOREGROUND
             └─16263 /usr/sbin/httpd -DFOREGROUND
               └─16265 /usr/sbin/httpd -DFOREGROUND
                 └─16266 /usr/sbin/httpd -DFOREGROUND
                   └─16269 /usr/sbin/httpd -DFOREGROUND
```

(рис. 2. Проверка работы веб-сервера)

С помощью команды “ps auxZ | grep httpd” определили контекст безопасности веб-сервера Apache - httpd_t



```
aarushisingh@vbox:~$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 16262 0.1 0.2 19220 12000 ?
Ss 01:22 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16263 0.0 0.1 18804 5560 ?
S 01:22 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16265 0.0 0.2 978228 8100 ?
Sl 01:22 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16266 0.0 0.2 1109364 8376 ?
Sl 01:22 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16269 0.0 0.2 978228 8100 ?
Sl 01:22 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aarushi+ 16790 0.0 0.0 23
0340 2156 pts/1 S+ 01:25 0:00 grep --color=auto httpd
aarushisingh@vbox:~$
```

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

Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off”

```
aarushisingh@vbox:~  
aarushisingh@vbox:~$ sestatus -b httpd  
SELinux status:                enabled  
SELinuxfs mount:                /sys/fs/selinux  
SELinux root directory:        /etc/selinux  
Loaded policy name:             targeted  
Current mode:                   permissive  
Mode from config file:          enforcing  
Policy MLS status:              enabled  
Policy deny_unknown status:     allowed  
Memory protection checking:     actual (secure)  
Max kernel policy version:      33  
  
Policy booleans:  
abrt_anon_write                  off  
abrt_handle_event                on  
abrt_upload_watch_anon_write     on  
antivirus_can_scan_system       off  
antivirus_use_jit               off  
auditadm_exec_content            on  
authlogin_nsswitch_use_ldap      off  
authlogin_radius                off  
authlogin_yubikey                off  
awstats_purge_apache_log_files  off  
boinc_execmem                    on  
cdrecord_read_content            off
```

(рис. 4.1. Текущее состояние переключателей SELinux)

```
aarushisingh@vbox:~  
webadm_read_user_files           off  
wine_mmap_zero_ignore            off  
xdm_bind_vnc_tcp_port            off  
xdm_exec_bootloader              off  
xdm_manage_bootloader            on  
xdm_sysadm_login                 off  
xdm_write_home                   off  
xen_use_nfs                      off  
xend_run_blktp                   on  
xend_run_qemu                    on  
xguest_connect_network           on  
xguest_exec_content              on  
xguest_mount_media               on  
xguest_use_bluetooth             on  
xserver_clients_write_xshm       off  
xserver_execmem                  off  
xserver_object_manager            off  
zabbix_can_network               off  
zabbix_run_sudo                  off  
zarafa_setrlimit                 off  
zebra_write_config               off  
zoneminder_anon_write            off  
zoneminder_run_sudo              off  
aarushisingh@vbox:~$
```

(рис. 4.2. Текущее состояние переключателей SELinux)

Посмотрели статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 5100

```
aarushisingh@vbox:~  
* Waiting in queue...  
* Downloading packages...  
* Requesting data...  
* Testing changes...  
* Installing updates...  
* Installing packages...  
* Cleaning up packages...  
* Installing packages...  
Statistics for policy file: /sys/fs/selinux/policy  
Policy Version: 33 (MLS enabled)  
Target Policy: selinux  
Handle unknown classes: allow  
Classes: 134 Permissions: 460  
Sensitivities: 1 Categories: 1024  
Types: 5236 Attributes: 262  
Users: 8 Roles: 15  
Booleans: 362 Cond. Expr.: 395  
Allow: 67517 Neverallow: 0  
Auditallow: 174 Dontaudit: 8767  
Type_trans: 271197 Type_change: 80  
Type_member: 38 Range_trans: 5643  
Role allow: 40 Role_trans: 411  
Constraints: 70 Validatetrans: 0  
MLS Constrains: 72 MLS Val. Tran: 0  
Permissives: 16 Polcap: 6
```

(рис. 5. Статистика по политике)

С помощью команды “ls -lZ /var/www” посмотрели файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определили, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html

```
aarushisingh@vbox:~$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 0 Aug 1 2  
024 cgi-bin  
drwxr-xr-x. 1 root root system_u:object_r:httpd_sys_content_t:s0 0 Aug 1 2  
024 html  
aarushisingh@vbox:~$
```

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

От имени суперпользователя создали html-файл /var/www/html/test.html. Контекст созданного файла - httpd_sys_content_t

```
root@vbox:/home/aarushisingh# nano /var/www/html/test.html  
root@vbox:/home/aarushisingh# nano /var/www/html/test.html  
root@vbox:/home/aarushisingh# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 May 3 0  
1:44 test.html  
root@vbox:/home/aarushisingh#
```

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

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

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

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

Изучив справку `man httpd_selinux`, выяснили, 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). Изменили контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверили, что контекст поменялся

```
aarushisingh@vbox:~$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
aarushisingh@vbox:~$ 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
aarushisingh@vbox:~$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for aarushisingh:
aarushisingh@vbox:~$ sudo chcon -t samba_share_t /var/www/html/test.html
aarushisingh@vbox:~$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
aarushisingh@vbox:~$
```

(рис. 9. Изменение контекста)

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. к установленному ранее контексту процесс `httpd` не имеет доступа)

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

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

Командой “`ls -l /var/www/html/test.html`” убедились, что читать данный файл может любой пользователь. Просмотрели системный лог-файл веб-сервера Apache командой “`sudo tail /var/log/messages`”, отображающий ошибки

```
aarushisingh@vbox:~$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
aarushisingh@vbox:~$ sudo tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
aarushisingh@vbox:~$
```

(рис. 11. Просмотр log-файла)

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. Установка веб-сервера Apache на прослушивание TCP-порта 81)

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

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

```
aarushisingh@vbox:~$ systemctl restart httpd
aarushisingh@vbox:~$ tail -nl /var/log/messages
tail: invalid number of lines: 'l'
aarushisingh@vbox:~$ tail -nl /var/log/messages
tail: invalid number of lines: 'l'
aarushisingh@vbox:~$ tail -nl /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
aarushisingh@vbox:~$ sudo tail -nl /var/log/messages
[sudo] password for aarushisingh:
tail: cannot open '/var/log/messages' for reading: No such file or directory
aarushisingh@vbox:~$
```

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

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. Содержание файла var/log/audit/audit.log)

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

Выполнили команду “semanage port -a -t http_port_t -p tcp 81” и убедились, что порт TCP-81 установлен. Проверили список портов командой “semanage port -l | grep http_port_t”, убедились, что порт 81 есть в списке и запускаем веб-сервер Apache снова

```
aarushisingh@vbox:~$ sudo semanage port -l | grep http_port_t
sudo: semanage: command not found
aarushisingh@vbox:~$ sudo semanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443,
9000
http_port_t          udp      80, 443
pegasus_http_port_t  tcp      5988
aarushisingh@vbox:~$ stsemctl restart httpd
bash: stsemctl: command not found...
aarushisingh@vbox:~$ systemctl restart httpd
aarushisingh@vbox:~$ curl ifconfig.me
109.252.181.95aarushisingh@vbox:~$ status httpd
status: command not found...
aarushisingh@vbox:~$ systemctl restart httpd
aarushisingh@vbox:~$ curl ifconfig.me
109.252.181.95aarushisingh@vbox:~$
```

(рис. 15. Проверка установки порта 81)

Вернули контекст “httpd_sys_content_t” файлу “/var/www/html/test.html” командой “chcon -t httpd_sys_content_t /var/www/html/test.html” и после этого попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидели содержимое файла - слово “test”

```
109.252.181.95aarushisingh@vbox:~$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
aarushisingh@vbox:~$ ls -Z /var/www/html.test.html
ls: cannot access '/var/www/html.test.html': No such file or directory
aarushisingh@vbox:~$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
aarushisingh@vbox:~$
```

(рис. 16. Возвращение исходного контекста файлу)

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

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

Исправили обратно конфигурационный файл apache, вернув “Listen 80”. Попытались удалить привязку http_port к 81 порту командой “semanage port -d -t http_port_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить

```
aarushisingh@vbox:~$ nano /etc/httpd/conf/httpd.conf
aarushisingh@vbox:~$ sudo semanage port -d -t http_port_t -p tcp 81
aarushisingh@vbox:~$ sudo semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
http_port_t      udp      80, 443
pegasus_http_port_t  tcp      5988
aarushisingh@vbox:~$ cat /etc/httpd/conf/httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
```

(рис. 18. Возвращение Listen 80 и попытка удалить порт 81)

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

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

(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>