Лабораторная работа №6

Мандатное разграничение прав в Linux

Хусаинова Д.А. Группа НПИбд-02-21

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 1/2

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. 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.

Теоретическое введение 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).

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.

Выполнение лабораторной работы

getenforce и sestatus

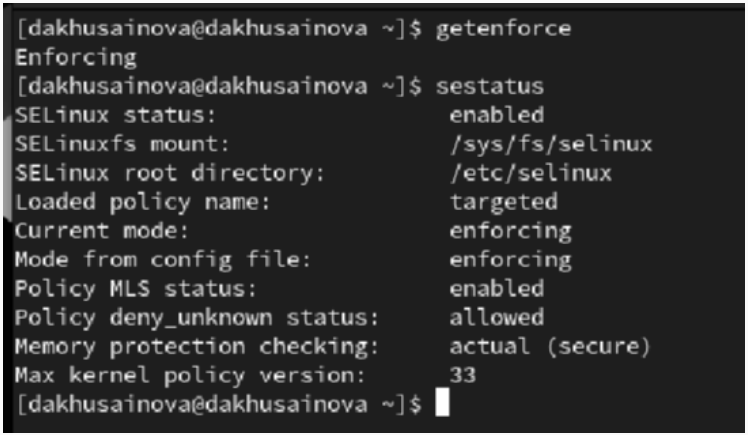
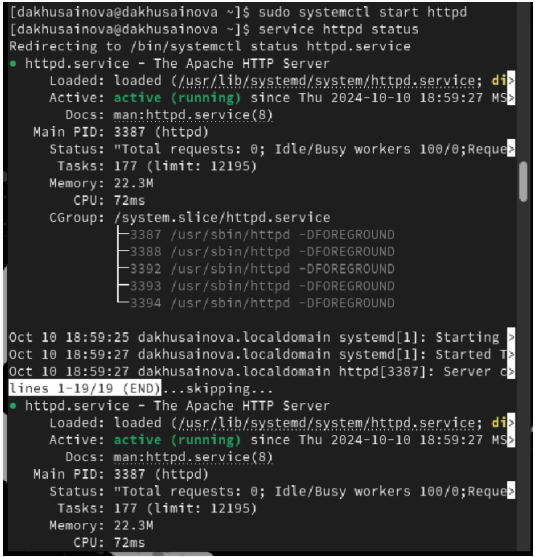
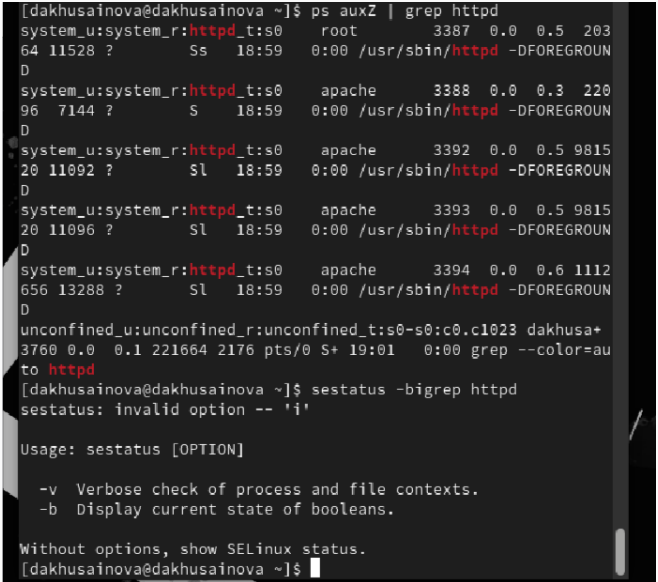


Рис. 1: getenforce и sestatus

status


[dakhusainova@dakhusainova ~]$ sudo systemctl start httpd
[dakhusainova@dakhusainova ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; di>
Active: active (running) since Thu 2024-10-10 18:59:27 MS>
Docs: man:httpd.service(8)
Main PID: 3387 (httpd)
Status: "Total requests: 0; Idle/Busy workers 100/0;Reque>
Tasks: 177 (limit: 12195)
Memory: 22.3M
CPU: 72ms
CGroup: /system.slice/httpd.service
├─3387 /usr/sbin/httpd -DFOREGROUND
├─3388 /usr/sbin/httpd -DFOREGROUND
├─3392 /usr/sbin/httpd -DFOREGROUND
├─3393 /usr/sbin/httpd -DFOREGROUND
└─3394 /usr/sbin/httpd -DFOREGROUND
Oct 10 18:59:25 dakhusainova.localdomain systemd[1]: Starting >
Oct 10 18:59:27 dakhusainova.localdomain systemd[1]: Started T>
Oct 10 18:59:27 dakhusainova.localdomain httpd[3387]: Server c>
lines 1-19/19 (END)...skipping...
● httpd.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/httpd.service; di>
Active: active (running) since Thu 2024-10-10 18:59:27 MS>
Docs: man:httpd.service(8)
Main PID: 3387 (httpd)
Status: "Total requests: 0; Idle/Busy workers 100/0;Reque>
Tasks: 177 (limit: 12195)
Memory: 22.3M
CPU: 72ms

ps auxZ | grep httpd and sestatus



Определение типа файлов

```
[dakhusainova@dakhusainova ~]$ 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:             5145    Attributes:          259
  Users:                8    Roles:                15
  Booleans:           356    Cond. Expr.:         388
  Allow:            65500    Neverallow:            0
  Auditallow:         176    Dontaudit:          8682
  Type_trans:      271770    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:          4    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
[dakhusainova@dakhusainova ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec
_t:s0 6 Aug  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s
0     6 Aug  8 19:30 html
[dakhusainova@dakhusainova ~]$ ls -lZ /var/www/html
total 0
```

создание файла

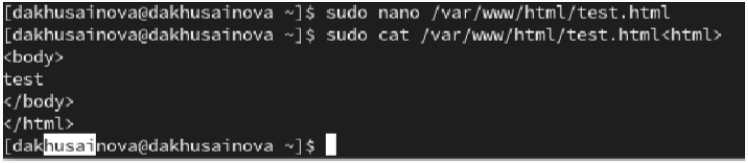


Рис. 5: создание файла

проверка контекста

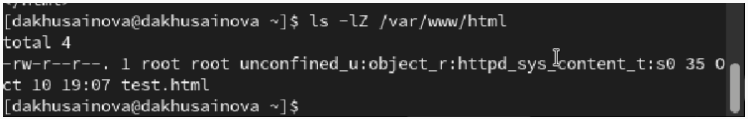


Рис. 6: проверка контекста

обращение к файлу

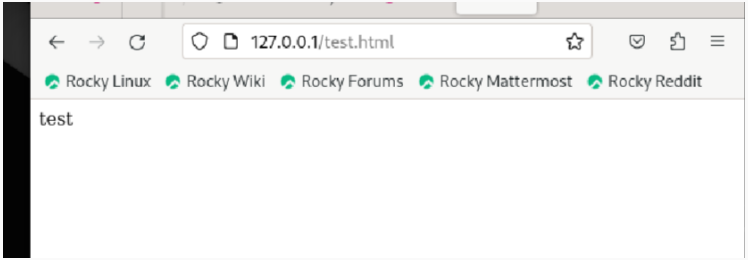
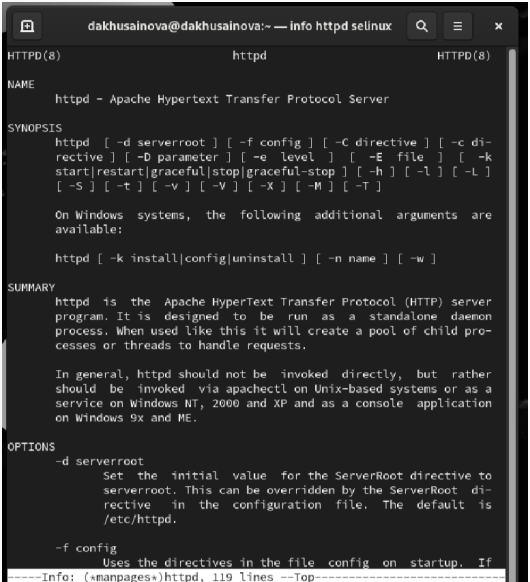


Рис. 7: обращение к файлу

man httpd_selinux



проверка контекста файла

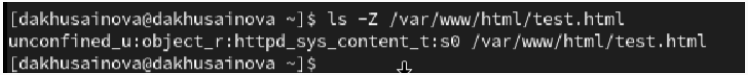


Рис. 9: проверка контекста файла

Изменение контекста файла

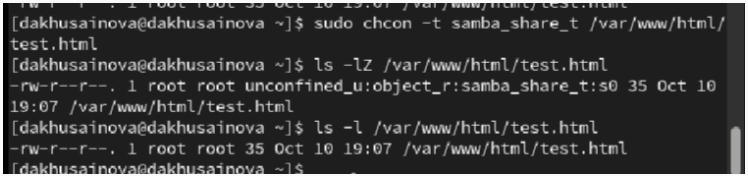


Рис. 10: Изменение контекста файла

сообщение об ошибке

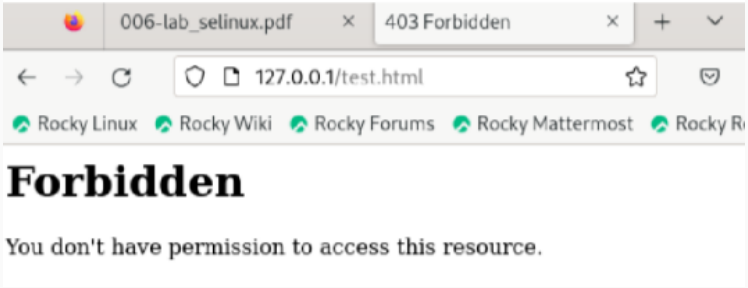


Рис. 11: You don’t have permission to access

просмотр логов

```
[dakhusainova@dakhusainova ~]$ sudo tail /var/log/messages
Oct 10 19:21:46 dakhusainova systemd[1]: Started SETroubleshoot daemon fo
r processing new SELinux denial logs.
Oct 10 19:21:46 dakhusainova setroubleshoot[4506]: failed to retrieve rpm
 info for path '/var/www/html/test.html':
Oct 10 19:21:46 dakhusainova systemd[1]: Created slice Slice /system/dbus
-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 10 19:21:46 dakhusainova systemd[1]: Started dbus-:1.1-org.fedoraproj
ect.SetroubleshootPrivileged@0.service.
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing
/usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
For complete SELinux messages run: sealert -l 68690a52-e372-4bef-8939-553
277261788
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing
/usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#
012#012*****  Plugin restorecon (92.2 confidence) suggests   **********
**********#012#012If you want to fix the label. #012/var/www/html/test.
html default label should be httpd_sys_content_t.#012Then you can run res
torecon. The access attempt may have been stopped due to insufficient per
missions to access a parent directory in which case try to change the fol
lowing command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/
test.html#012#012*****  Plugin public_content (7.83 confidence) suggests
  **********#012#012If you want to treat test.html as public co
ntent#012Then you need to change the label on test.html to public_content
_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.ht
ml'#012#012*****  Plugin catchall (1.41 confidence) suggests   **********
**********#012#012If you believe that httpd should be allowed getat
tr access on the test.html file by default.#012Then you should report thi
s as a bug.#012You can generate a local policy module to allow this acces
s.#012Do#012allow this access for now by executing:#012# ausearch -c 'htt
pd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#0
12
Oct 10 19:21:47 dakhusainova setroubleshoot[4506]: SELinux is preventing
```

замена порта

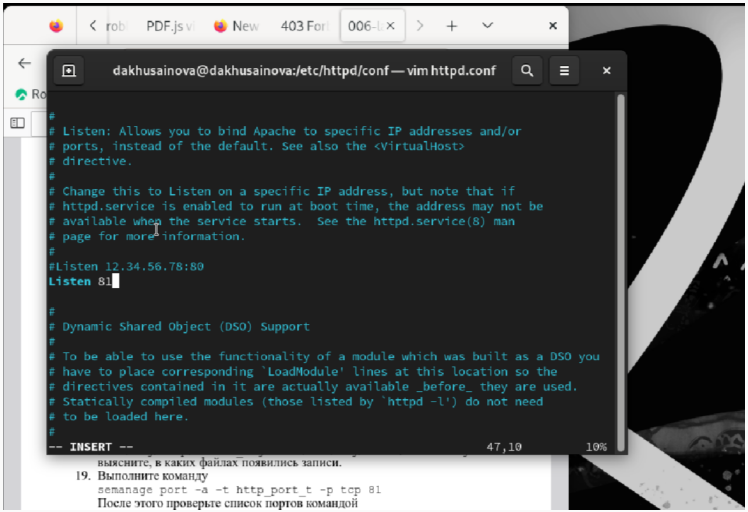


Рис. 13: замена порта

сбой

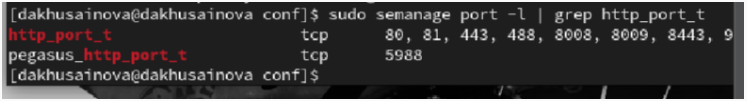


Рис. 14: сбой

удаление файла

Рис. 15: удаление файла

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] Права доступа:
https://codechick.io/tutorials/unix-linux/unix-linux-permissions