Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Морозов Михаил Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

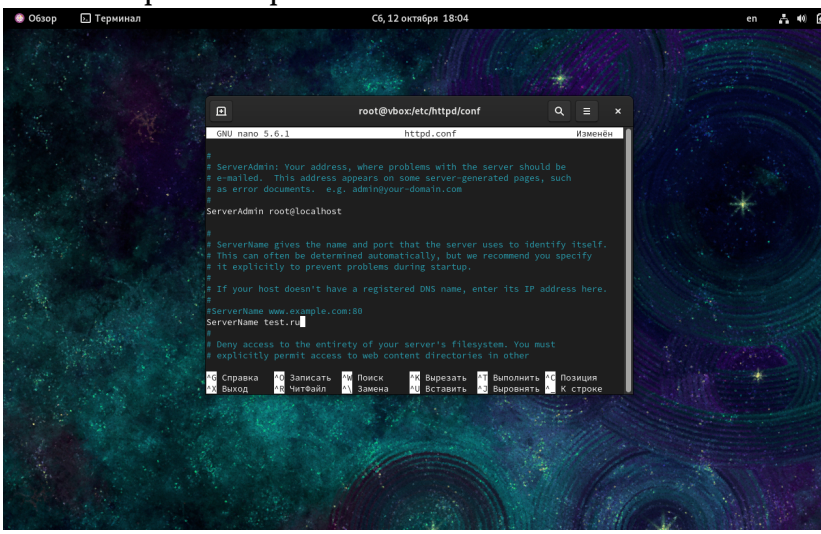
2 Теоретическое введение

В SELinux права доступа определяются самой системой при помощи специально определённых политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux: через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux. Две других формы контроля доступа — доступ на основе ролей и на основе многоуровневой системы безопасности. [1]

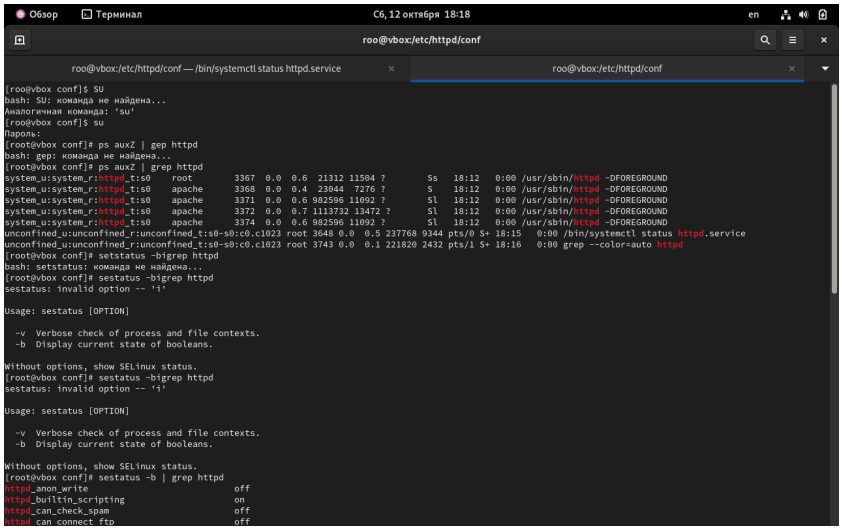
3 Выполнение лабораторной работы

Убедимся, что SELinux работает в режиме enforcing политики targeted. Обратимся к веб-серверу и убедимся, что он работает. Найдем apache в списке процессов. Посмотрим статистику по политике. Определим тип файлов и директорий в /var/www. Посмотрим список пользователей. Создадим от имени root файл в /var/www/html. Попробуем посмотреть файл в браузере. Изменим контекст файла. Добавим на прослушивание порт 81. Вернем все как было.

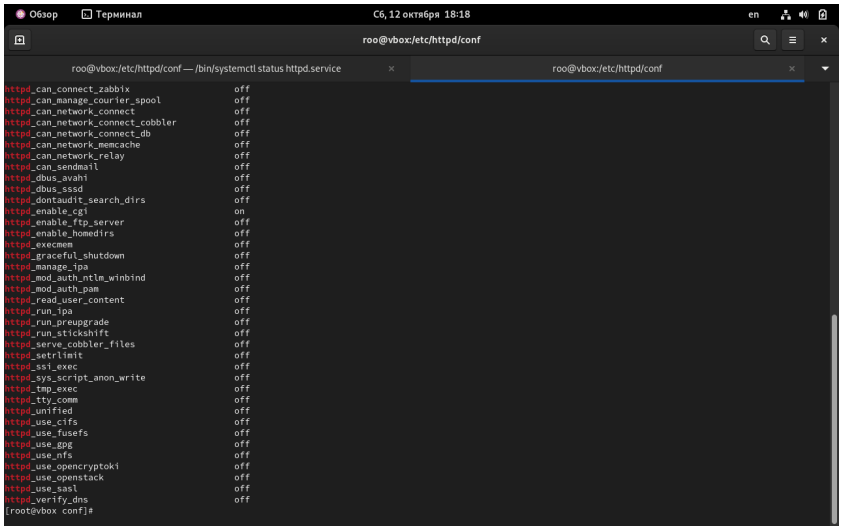
Результаты работы команд 1 (рис. **??**)



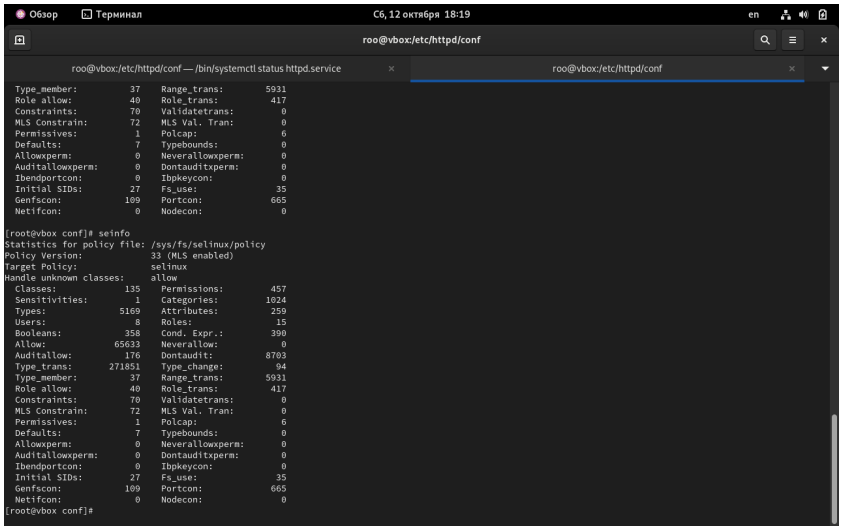
2 (рис. **??**)



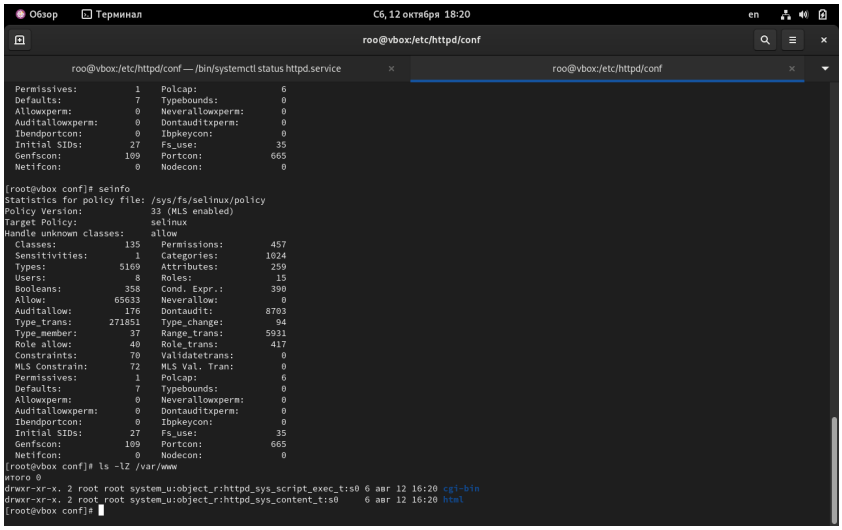
3 (рис. **??**)



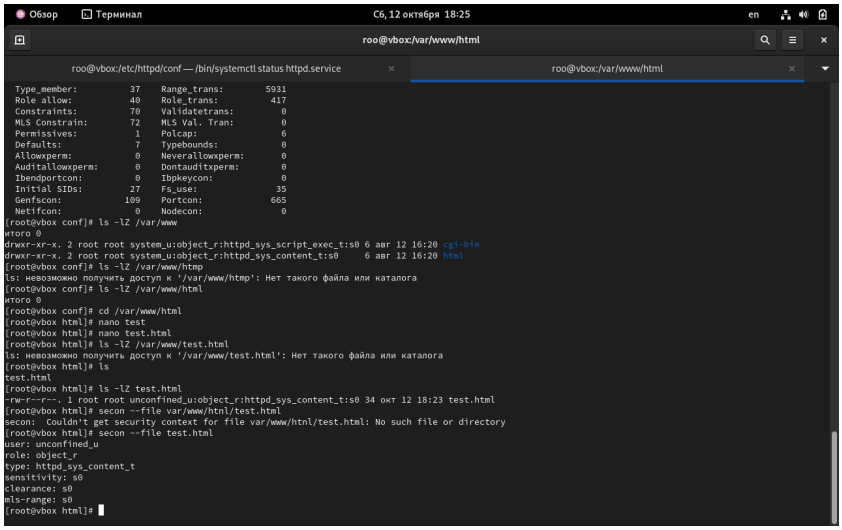
4 (рис. **??**)



5 (рис. **??**)


Обзор
Терминал
Сб, 12 октября 18:20
en
roo@vbox:/etc/httpd/conf
roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
roo@vbox:/etc/httpd/conf
Permissives: 1 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
[root@vbox conf]# 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: 5169 Attributes: 259
Users: 8 Roles: 15
Booleans: 358 Cond. Expr.: 390
Allow: 65633 Neverallow: 0
Auditallow: 176 Dontaudit: 8703
Type_trans: 271851 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: 1 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
[root@vbox conf]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 12 16:20 html
[root@vbox conf]#

6 (рис. **??**)


Обзор
Терминал
Сб, 12 октября 18:25
en
roo@vbox:/var/www/html
roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
roo@vbox:/var/www/html
Type_member: 37 Range_trans: 5931
Role allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 1 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
[root@vbox conf]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 12 16:20 html
[root@vbox conf]# ls -lZ /var/www/htmp
ls: невозможно получить доступ к '/var/www/htmp': Нет такого файла или каталога
[root@vbox conf]# ls -lZ /var/www/html
итого 0
[root@vbox conf]# cd /var/www/html
[root@vbox html]# nano test
[root@vbox html]# nano test.html
[root@vbox html]# ls -lZ /var/www/test.html
ls: невозможно получить доступ к '/var/www/test.html': Нет такого файла или каталога
[root@vbox html]# ls
test.html
[root@vbox html]# ls -lZ test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 окт 12 18:23 test.html
[root@vbox html]# secon --file var/www/html/test.html
secon: Couldn't get security context for file var/www/html/test.html: No such file or directory
[root@vbox html]# secon --file test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[root@vbox html]#

4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Sticky bit [Электронный ресурс]. Wikimedia Foundation, 2024. URL: https://ru.wikipedia.org/wiki/Sticky_bit.