

Отчет по лабораторной работе №6

Жиронкин Павел Влдимирович НПИбд-01-18¹

Информационная Безопасность–2021, 22 ноября, 2021, Москва,
Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

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

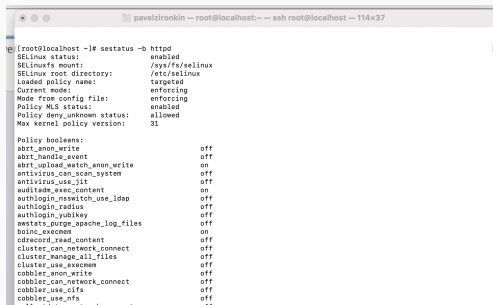
Задание к лабораторной работе

Лабораторная работа подразумевает выполнение последовательно необходимых действий, чтобы развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Процесс выполнения лабораторной работы

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`
2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status`.
3. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности.

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратил внимание, что многие из них находятся в положении «off». (рис. 1).



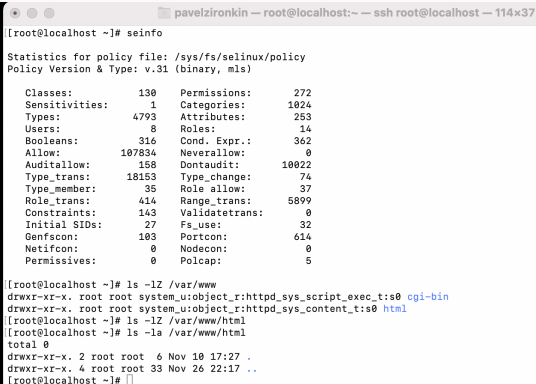
```
(root@localhost ~)# sestatus -b httpd
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Max kernel policy version:     31

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
audited_exec_content           on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmon                  on
cdrecord_read_content           off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmon            off
cobbler_anon_write              off
cobbler_can_network_connect     off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_to_network_connect    off
```

Рис. 1: Просмотр состояние переключателей SELinux для Apache

5. Посмотрел статистику по политике с помощью команды `seinfo`, также определил множество пользователей(8), ролей(14), типов(4793). Определил тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`. Определил тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Определил круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. (рис. 2).

Процесс выполнения



A terminal window titled 'pavelzironkin — root@localhost:~ — ssh root@localhost — 114x37'. The user runs 'seinfo' to get statistics for the policy file '/sys/fs/selinux/policy'. The output shows various counts for classes, sensitivities, types, users, booleans, allow rules, audit allow rules, type transitions, type members, role transitions, constraints, initial SIDs, genfscon, netifcon, permissions, categories, attributes, roles, conditional expressions, neverallow rules, dontaudit rules, type changes, role allows, range transitions, validate transitions, fs_use, portcon, nodecon, and polcap. Then, the user runs 'ls -lZ /var/www' showing SELinux contexts for CGI binaries and HTML files. Finally, the user runs 'ls -la /var/www/html' showing file permissions and timestamps for the HTML directory.

```
[root@localhost ~]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130   Permissions:      272
Sensitivities:    1     Categories:      1024
Types:           4793   Attributes:      253
Users:           8     Roles:           14
Booleans:        316   Cond. Expr.:     362
Allow:           107834 Neverallow:       0
Auditallow:      158   Dontaudit:       10022
Type_trans:      18153 Type_change:      74
Type_member:     35    Role_allow:      37
Role_trans:      414   Range_trans:     5899
Constraints:     143   Validatetrans:   0
Initial SIDs:    27    Fs_use:          32
Genfscon:        103   Portcon:         614
Netifcon:        0     Nodecon:         0
Permissives:     0     Polcap:          5

[root@localhost ~]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@localhost ~]# ls -lZ /var/www/html
[root@localhost ~]# ls -la /var/www/html
total 0
drwxr-xr-x. 2 root root 6 Nov 10 17:27 .
drwxr-xr-x. 4 root root 33 Nov 26 22:17 ..
[root@localhost ~]#
```

Рис. 2: Получение информации

6. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл
`/var/www/html/test.html`
7. Проверил контекст созданного файла.
`httpd_sys_content_t`
8. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедился, что файл был успешно отображён.
9. Проверил контекст файла командой: `ls -Z /var/www/html/test.html`

10. Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверил, что контекст поменялся.
11. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получили сообщение об ошибке.
12. Проанализировал ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл

13. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`). Для этого в файле `/etc/httpd/httpd.conf` нашла строчку `Listen 80` и заменил её на `Listen 81`.
14. Проанализировал лог-файлы. Просмотрел файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`.

15. Выполнил команду: `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов командой: `semanage port -l | grep http_port_t`. Убедился, что порт 81 появился в списке. (рис. 3).



```
pavelzironkin — root@localhost:/etc/httpd/conf — ssh root@localhost — 116x43
[root@localhost conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost conf]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@localhost conf]#
```

Рис. 3: Выполнение и проверка

16. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test»
17. Исправил обратно конфигурационный файл `apache`, вернув `Listen80`.
18. Удалил привязку `http_port_t` к 81 порту.
19. Удалил файл `/var/www/html/test.html`.

Выводы по проделанной работе

На основе проделанной работы развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.