Лабораторная работа № 6

Мандатное разграничение прав в Linux

Абу Сувейлим Мухаммед Мунифович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Задание

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности [1]

3 Выполнение лабораторной работы

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. 3.1).

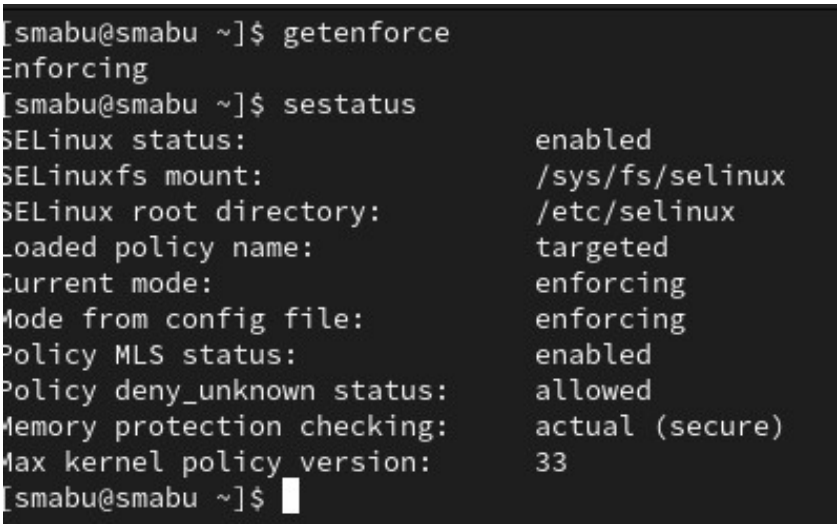

Рис. 3.1: Коианда getenforce

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или /etc/rc.d/init.d/httpd status Если не работает, запустите его так же, но с параметром start. (рис. 3.2):

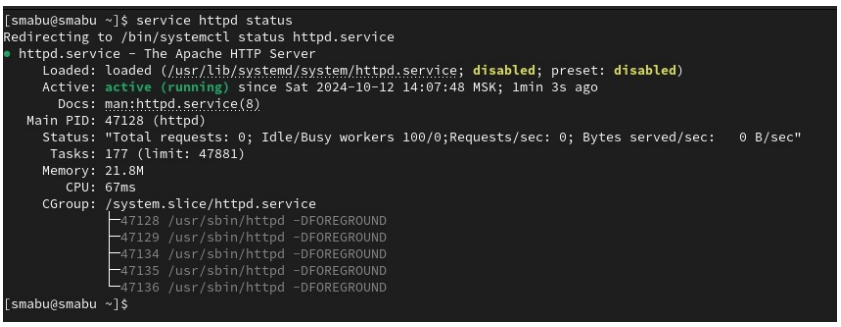

Рис. 3.2: Коианда service httpd status

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd (рис. 3.3):

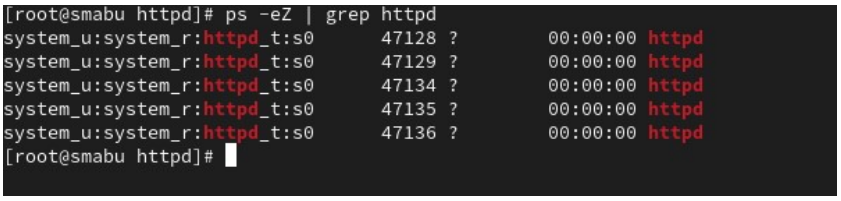

Рис. 3.3: Коианда ps -eZ | grep httpd

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды (рис. 3.4):

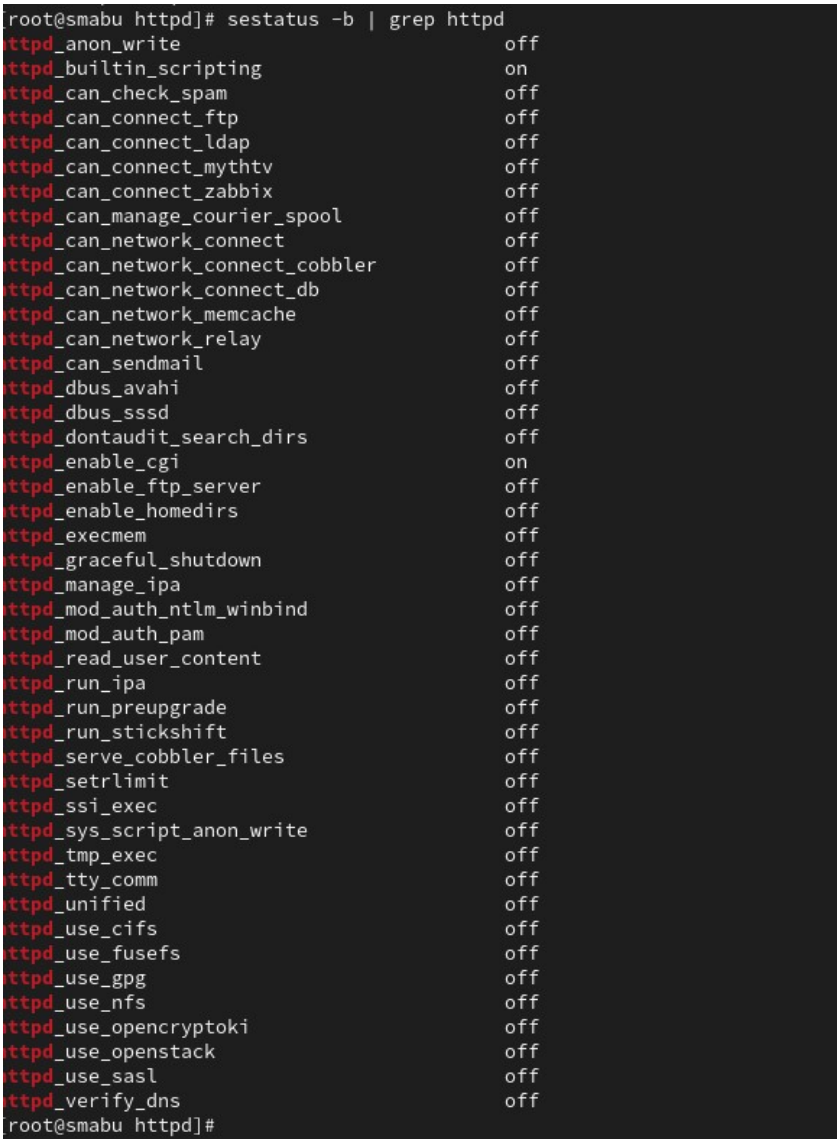

Рис. 3.4: Коианда sestatus -b | grep httpd

Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. 3.5):

```
[root@smabu httpd]# 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:           2    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@smabu httpd]#
```

Рис. 3.5: Коианда seinfo

Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www (рис. 3.6):

```
[root@smabu httpd]# 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@smabu httpd]# ls -lZ /var/www/html
итого 0
[root@smabu httpd]#
```

Рис. 3.6: Коианда ls -lZ /var/www

ОСоздайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 3.7):

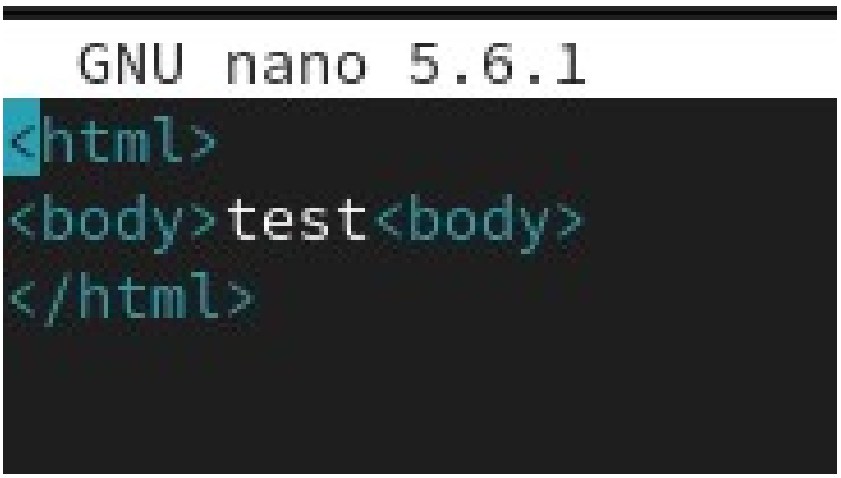

Рис. 3.7: html-файл test.html

Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображё (рис. 3.8):

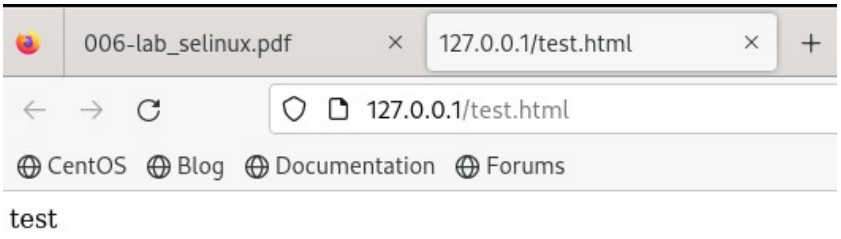

Рис. 3.8: html-файл test.html 2

Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.htm (рис. 3.9):

Рис. 3.9: Коианда man httpd

Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t (рис. 3.10):

```
[root@smabu httpd]# chcon -t samba_share_t /var/www/html/test.html
[root@smabu httpd]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@smabu httpd]#
```

Рис. 3.10: Коианда chcon

После этого проверьте, что контекст поменялся. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server. (рис. 3.11):

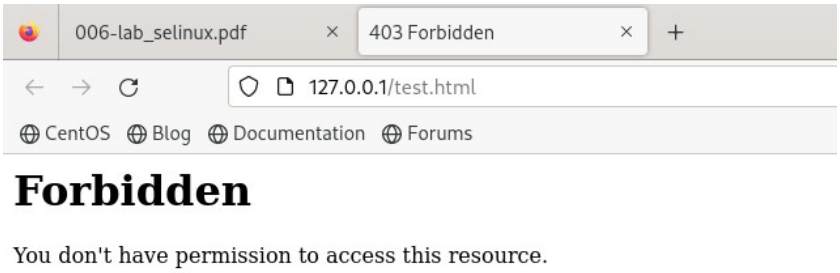

Рис. 3.11: Ошибка Forbidden

Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (рис. 3.12):

Рис. 3.12: Команда ls -l /var/www/html/test.html

Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в фай-

ле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. 3.13):

Рис. 3.13: Лог-файлы

Выполните команду semanage port -a -t http_port_t -p tcp 81 После этого проверьте список портов командой semanage port -l | grep http_port_t Убедитесь, что порт 81 появился в списке (рис. 3.14):

Рис. 3.14: Команда semanage

Верните 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 попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Исправьте обратно конфигурационный файл apache, вернув Listen 80. Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и

проверьте, что порт 81 удалён. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. 3.15):

Рис. 3.15: Команда rm /var/www/html/test.html

4 Выводы

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

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.