

Отчёт по лабораторной работе №6

Знакомство с SELinux

Виноградова Варвара Станиславовна НФИбд-01-18

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Подготовка	5
2.2	Изучение механики SetUID	5
3	Выводы	11
	Список литературы	12

List of Figures

2.1	запуск http	6
2.2	контекст безопасности http	6
2.3	переключатели SELinux для http	6
2.4	создание html-файла и доступ по http	7
2.5	ошибка доступа после изменения контекста	8
2.6	лог ошибок	9
2.7	переключение порта	9
2.8	доступ по http на 81 порт	10

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. 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`.

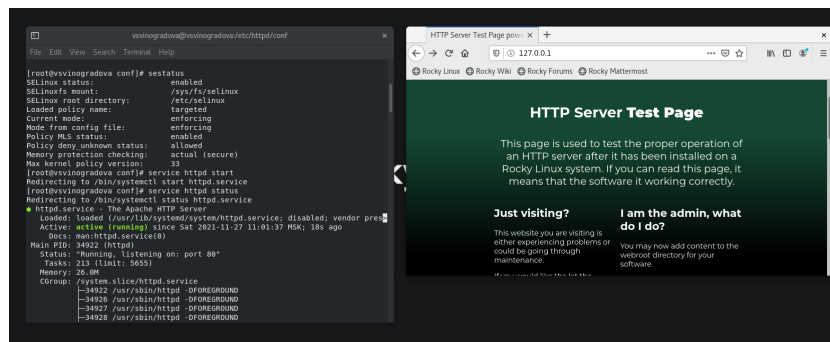


Figure 2.1: запуск http

3. 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`

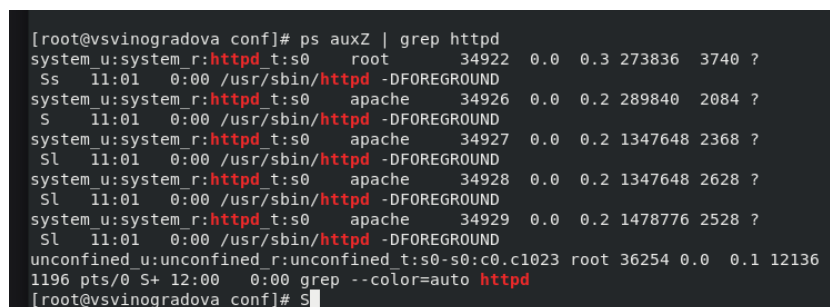


Figure 2.2: контекст безопасности http

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`. Обратите внимание, что многие из них находятся в положении «off».



Figure 2.3: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы может только root.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания: `Test`
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

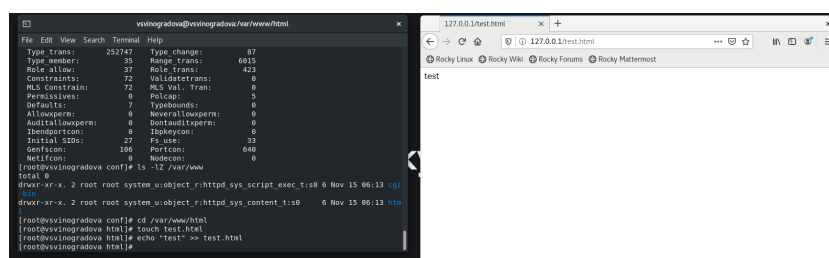


Figure 2.4: создание html-файла и доступ по http

12. 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.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.

13. 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`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.
14. 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.` При изменении контекста файл стал считаться чужим для `http` и программа не может его прочитать.

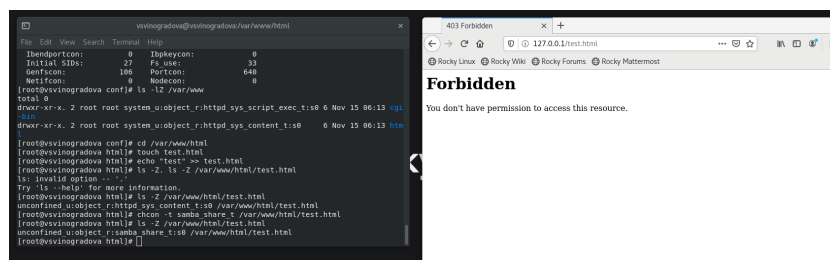
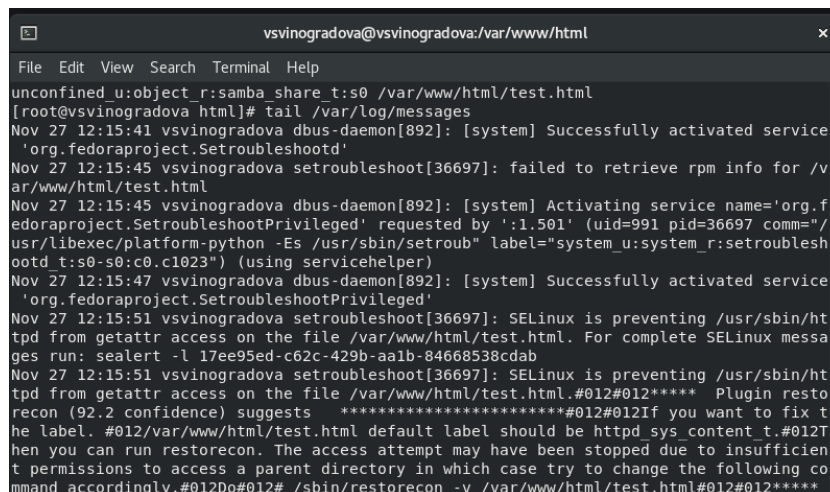


Figure 2.5: ошибка доступа после изменения контекста

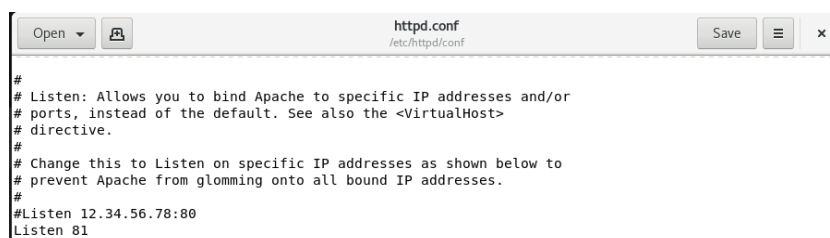
15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы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



```
unconfined u:object_r:samba_share t:s0 /var/www/html/test.html
[root@vsvinogradova html]# tail /var/log/messages
Nov 27 12:15:41 vsvinogradova dbus-daemon[892]: [system] Successfully activated service
'org.fedoraproject.SetroubleShoot'
Nov 27 12:15:45 vsvinogradova setroubleShoot[36697]: failed to retrieve rpm info for /v
ar/www/html/test.html
Nov 27 12:15:45 vsvinogradova dbus-daemon[892]: [system] Activating service name='org.f
edoraproject.SetroubleShootPrivileged' requested by ':1.501' (uid=991 pid=36697 comm="/
usr/libexec/platform-python -Es /usr/sbin/setroub label="system u:system_r:setroublesh
ootd t:s0-s0:c0.c1023") (using servicehelper)
Nov 27 12:15:47 vsvinogradova dbus-daemon[892]: [system] Successfully activated service
'org.fedoraproject.SetroubleShootPrivileged'
Nov 27 12:15:51 vsvinogradova setroubleShoot[36697]: SELinux is preventing /usr/sbin/ht
tpd from getattr access on the file /var/www/html/test.html. For complete SELinux messa
ges run: sealert -l 17ee95ed-c62c-429b-aa1b-84668538cdab
Nov 27 12:15:51 vsvinogradova setroubleShoot[36697]: SELinux is preventing /usr/sbin/ht
tpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin resto
recon (92.2 confidence) suggests *****#012#012If you want to fix t
he label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012T
hen you can run restorecon. The access attempt may have been stopped due to insufficien
t permissions to access a parent directory in which case try to change the following co
mmand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****
```

Figure 2.6: лог ошибок

16. Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81.

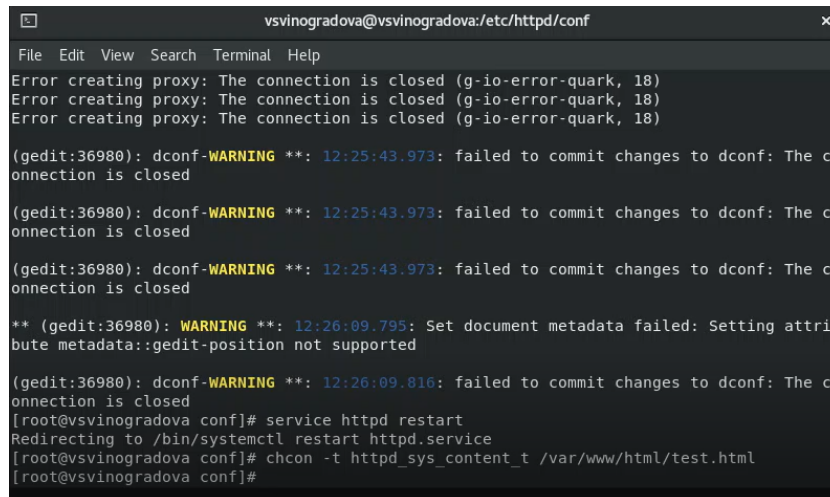


```
Open [icon] httpd.conf /etc/httpd/conf Save [icon] x
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Figure 2.7: переключение порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
18. Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите фай-
лы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и
выясните, в каких файлах появились записи.
19. Выполните команду semanage port -a -t http_port_t -p tcp 81 После этого про-
верьте список портов командой semanage port -l | grep http_port_t Убедитесь,
что порт 81 появился в списке.

20. Попробуйте запустить веб-сервер Apache ещё раз.
21. 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`. Вы должны увидеть содержимое файла — слово «test».



```
vsvinogradova@vsvinogradova:etc/httpd/conf
File Edit View Search Terminal Help
Error creating proxy: The connection is closed (g-io-error-quark, 18)
Error creating proxy: The connection is closed (g-io-error-quark, 18)
Error creating proxy: The connection is closed (g-io-error-quark, 18)
(gedit:36980): dconf-WARNING **: 12:25:43.973: failed to commit changes to dconf: The connection is closed
(gedit:36980): dconf-WARNING **: 12:25:43.973: failed to commit changes to dconf: The connection is closed
(gedit:36980): dconf-WARNING **: 12:25:43.973: failed to commit changes to dconf: The connection is closed
** (gedit:36980): WARNING **: 12:26:09.795: Set document metadata failed: Setting attribute metadata:gedit-position not supported
(gedit:36980): dconf-WARNING **: 12:26:09.816: failed to commit changes to dconf: The connection is closed
[root@vsvinogradova conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vsvinogradova conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vsvinogradova conf]#
```

Figure 2.8: доступ по http на 81 порт

22. Исправьте обратно конфигурационный файл apache, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

3 Выводы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.

Список литературы

1. SELinux в CentOS
2. Веб-сервер Apache