

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Ким Реачна

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
2.1	Подготовка	5
2.2	Изучение механики SetUID	5
3	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	getenforce и sestatus	6
2.2	запуск http	7
2.3	контекст безопасности http	7
2.4	переключатели SELinux для http	8
2.5	статистика по политике	9
2.6	создание html-файла и доступ по http	10
2.7	ошибка доступа после изменения контекста	11
2.8	лог ошибок	12
2.9	переключение порта	13
2.10	доступ по http на 81 порт	14

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`.

```
[kreachna@kreachna ~]$ getenforce
Enforcing
[kreachna@kreachna ~]$ sestatus
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
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[kreachna@kreachna ~]$ su
Password:
\[root@kreachna kreachna]# yum -y install httpd
Extra Packages for Enterprise Linux 9 - x86_64      56 kB/s | 17 kB      00:00
Extra Packages for Enterprise Linux 9 - x86_64      7.8 MB/s | 19 MB      00:02
Rocky Linux 9 - BaseOS                             7.3 kB/s | 4.1 kB      00:00
Rocky Linux 9 - BaseOS                             2.2 MB/s | 1.9 MB      00:00
Rocky Linux 9 - AppStream                          10 kB/s | 4.5 kB      00:00
Rocky Linux 9 - AppStream                          6.3 MB/s | 7.1 MB      00:01
Rocky Linux 9 - Extras                             7.1 kB/s | 2.9 kB      00:00
Dependencies resolved.
=====
Package                Architecture Version                Repository            Size
=====
Installing:
  httpd                 x86_64        2.4.53-11.el9_2.5     appstream              47 k
Installing dependencies:
```

Рис. 2.1: 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`.

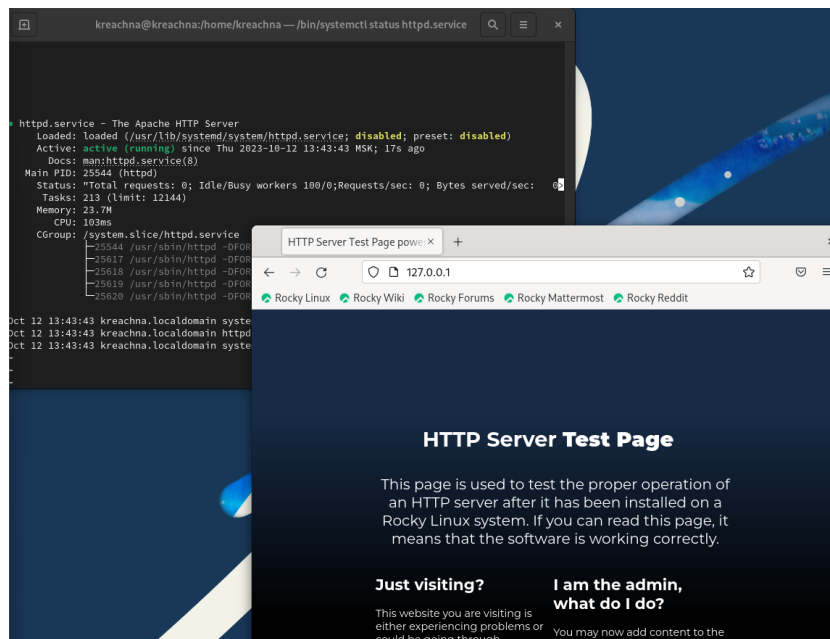


Рис. 2.2: запуск http

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`

```
[root@kreachna kreachna]# ps aux -Z | grep httpd
system_u:system_r:httpd_t:s0 root 25544 0.0 0.4 20328 9528 ? Ss 13:43 0:
00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 25617 0.0 0.2 21664 5932 ? S 13:43 0:
00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 25618 0.0 0.5 1538228 10376 ? Sl 13:43 0:
00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 25619 0.0 0.5 1669364 11696 ? Sl 13:43 0:
00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 25620 0.0 0.5 1538228 10304 ? Sl 13:43 0:
00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 44179 0.0 0.4 1538228 9808 ? Sl 13:45 0:
00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 44443 0.0 0.1 221796 2268 pts/0 S+ 1
3:48 0:00 grep --color=auto httpd
```

Рис. 2.3: 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».

```
[root@kreachna kreachna]# sestatus -b | grep httpd
httpd_anon_write           off
httpd_builtin_scripting    on
httpd_can_check_spam       off
httpd_can_connect_ftp      off
httpd_can_connect_ldap     off
httpd_can_connect_mythtv   off
httpd_can_connect_zabbix   off
httpd_can_manage_courier_spool off
httpd_can_network_connect  off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay    off
httpd_can_sendmail         off
httpd_dbus_avahi           off
httpd_dbus_sssd            off
httpd_dontaudit_search_dirs off
httpd_enable_cgi           on
httpd_enable_ftp_server    off
httpd_enable_homedirs      off
httpd_execmem              off
httpd_graceful_shutdown    off
httpd_manage_ipa           off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam         off
httpd_read_user_content    off
httpd_run_ipa              off
httpd_run_preupgrade        off
httpd_run_stickshift        off
httpd_serve_cobbler_files  off
httpd_setrlimit            off
httpd_ssi_exec             off
httpd_sys_script_anon_write off
httpd_tmp_exec             off
httpd_tty_comm             off
httpd_unified              off
httpd_use_cifs              off
httpd_use_fusefs           off
httpd_use_gpg              off
httpd_use_nfs              off
httpd_use_openscryptoki     off
httpd_use_openstack        off
httpd_use_sasl              off
httpd_verify_dns           off
[root@kreachna kreachna]#
```

Рис. 2.4: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.


```

* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...
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:               5118     Attributes:            258
Users:               8        Roles:                14
Booleans:            353     Cond. Expr.:          384
Allow:               65609    Neverallow:            0
Auditallow:          172     Dontaudit:             8591
Type_trans:          267951   Type_change:           87
Type_member:          35     Range_trans:           6164
Role allow:           38     Role_trans:            420
Constraints:          70     Validatetrans:         0
MLS Constrains:       72     MLS Val. Tran:         0
Permissives:          7      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:               660
Netifcon:             0      Nodecon:               0

```

Рис. 2.5: статистика по политике

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.

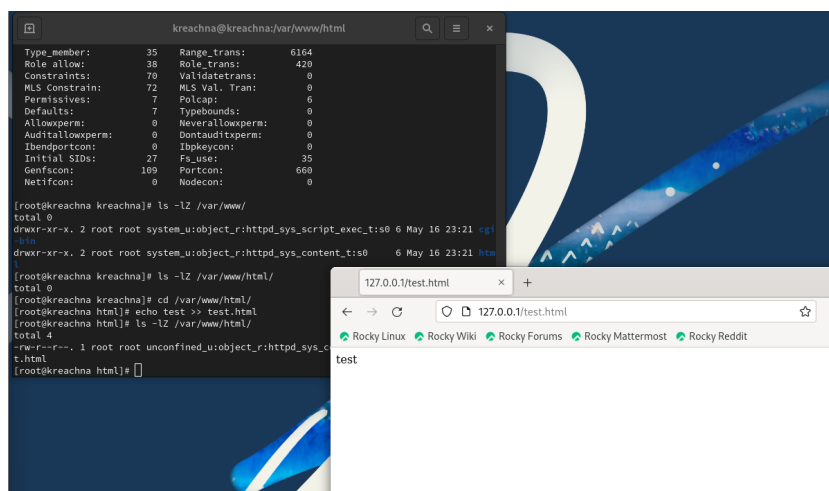


Рис. 2.6: создание html-файла и доступ по http

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.

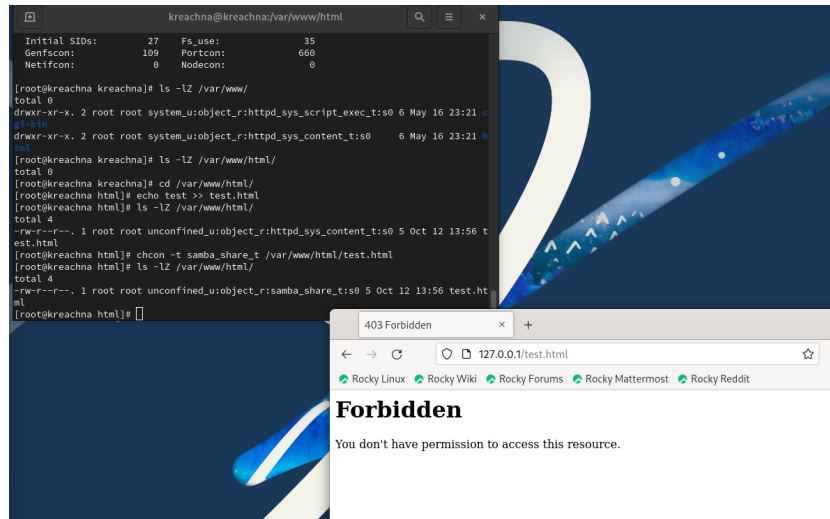


Рис. 2.7: ошибка доступа после изменения контекста

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.

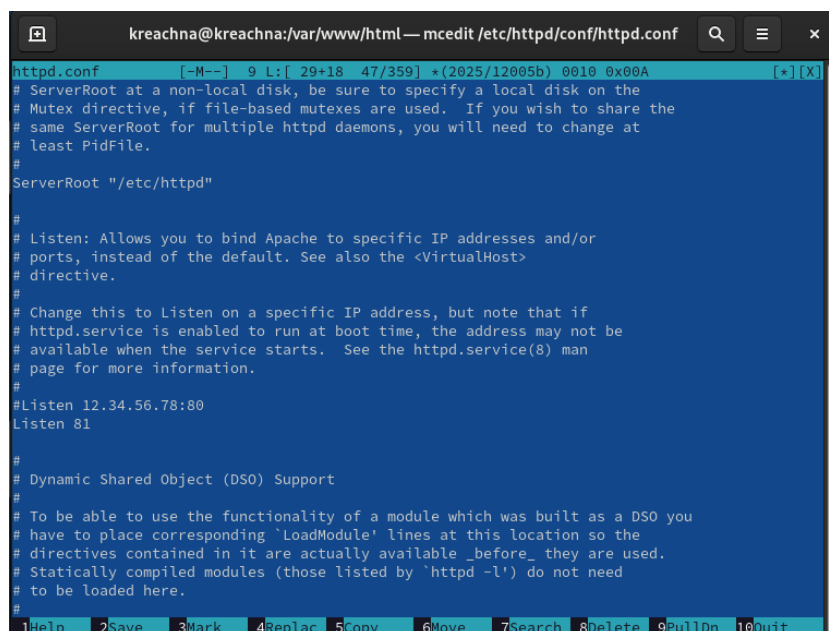
```

[root@kreachna html]# tail /var/log/messages
Oct 12 14:01:36 kreachna systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 12 14:01:36 kreachna systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 12 14:01:39 kreachna setroubleshoot[45010]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 6d951de3-8550-4aa4-bd1e-1ce25bc487fc
Oct 12 14:01:39 kreachna setroubleshoot[45010]: SELinux is preventing /usr/sbin/httpd from getting 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 restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following 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 content#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_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed to getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 14:01:39 kreachna setroubleshoot[45010]: SELinux is preventing /usr/sbin/httpd from getting 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 restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following 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 content#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_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed to getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 12 14:01:39 kreachna setroubleshoot[45010]: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 6d951de3-8550-4aa4-bd1e-1ce25bc487fc
Oct 12 14:01:49 kreachna systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 12 14:01:49 kreachna systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.425s CPU time.
Oct 12 14:01:49 kreachna systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 12 14:01:49 kreachna systemd[1]: setroubleshootd.service: Consumed 1.252s CPU time.

```

Рис. 2.8: 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.



```
httpd.conf [-M--] 9 L: [ 29+18 47/359] *(2025/12005b) 0010 0x00A [*] [X]
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# 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 a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
```

Рис. 2.9: 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 файлы `/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 проверьте 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».

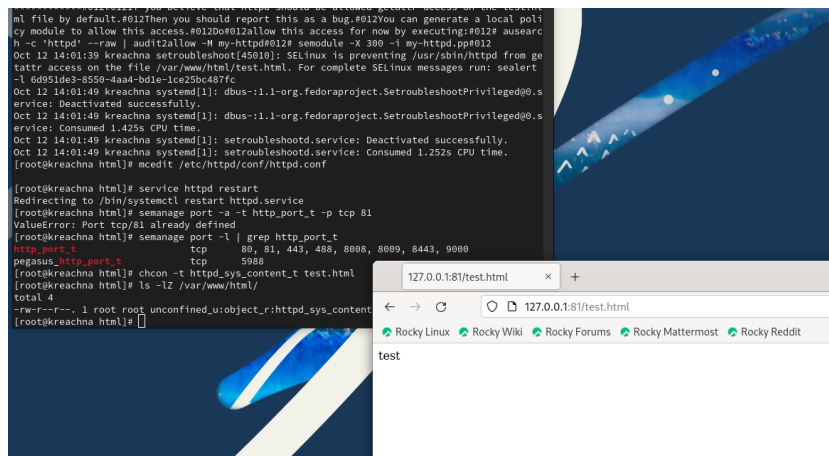


Рис. 2.10: доступ по http на 81 порт

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