Лабораторная работа №6

Мандатное разграничение прав в Linux

Калинина Кристина Сергеевна

Цель работы

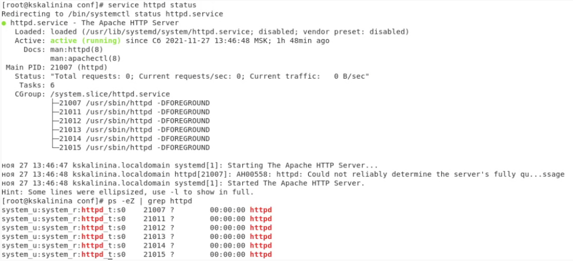
Цель работы

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

Выполнение

1. Выполнение лабораторной работы
2. Оформление отчета и презентации
3. Выгрузка видео на youtube и файлов на GitHub

Веб-сервис Apache

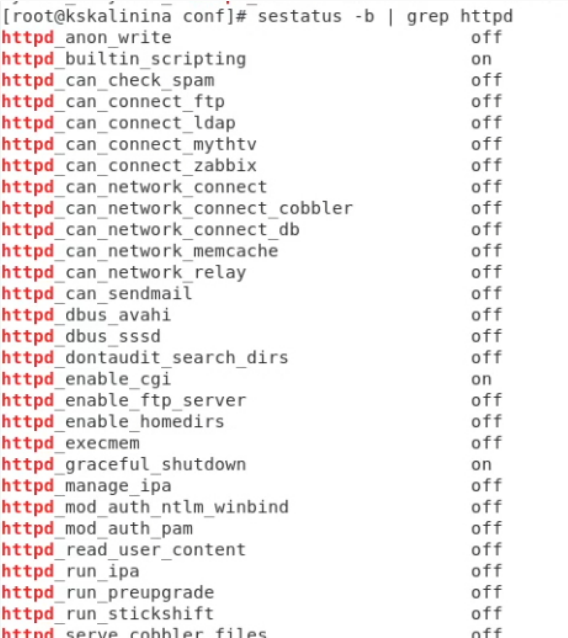


```
[root@kskalinina conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Сб 2021-11-27 13:46:48 MSK; 1h 48min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 21007 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─21007 /usr/sbin/httpd -DFOREGROUND
           ├─21011 /usr/sbin/httpd -DFOREGROUND
           ├─21012 /usr/sbin/httpd -DFOREGROUND
           ├─21013 /usr/sbin/httpd -DFOREGROUND
           ├─21014 /usr/sbin/httpd -DFOREGROUND
           └─21015 /usr/sbin/httpd -DFOREGROUND

ноя 27 13:46:47 kskalinina.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 13:46:48 kskalinina.localdomain httpd[21007]: AH00558: httpd: Could not reliably determine the server's fully qu...ssage
ноя 27 13:46:48 kskalinina.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@kskalinina conf]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0    21007 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21011 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21012 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21013 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21014 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0    21015 ?        00:00:00 httpd
```

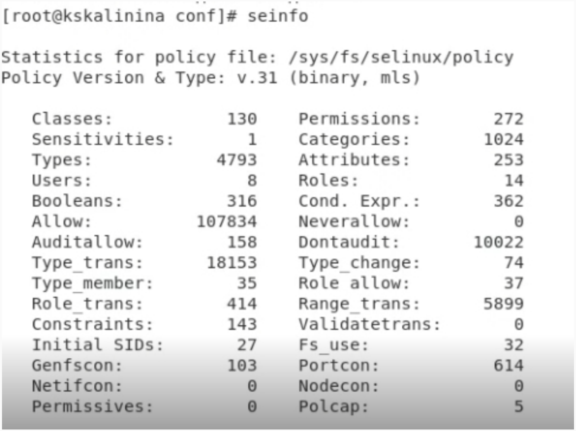
Figure 1: Проверка Apache

Состояние переключателей SELinux для Apache



```
[root@kskalinina conf]# 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_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                     on
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
```

Статистика по политике



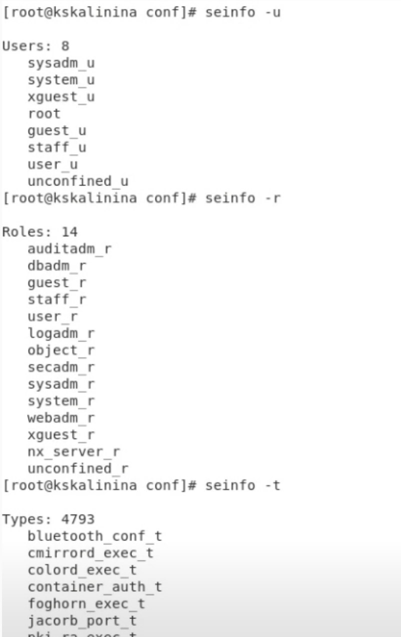
```
[root@kskalinina conf]# seinfo

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
```

Figure 3: Статистика по политике

Статистика по политике



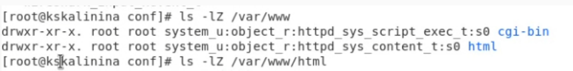
```
[root@kskalinina conf]# seinfo -u

Users: 8
   sysadm_u
   system_u
   xguest_u
   root
   guest_u
   staff_u
   user_u
   unconfined_u
[root@kskalinina conf]# seinfo -r

Roles: 14
   auditadm_r
   dbadm_r
   guest_r
   staff_r
   user_r
   logadm_r
   object_r
   secadm_r
   sysadm_r
   system_r
   webadm_r
   xguest_r
   nx_server_r
   unconfined_r
[root@kskalinina conf]# seinfo -t

Types: 4793
   bluetooth_conf_t
   cmirrord_exec_t
   colord_exec_t
   container_auth_t
   foghorn_exec_t
   jacorb_port_t
   pki_ra_exec_t
```

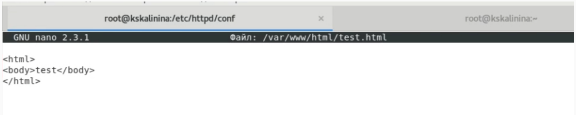
Просмотр информации о директориях “/var/www” и “/var/www/html”



```
[root@kskalinina conf]# 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@kskalinina conf]# ls -lZ /var/www/html
```

Figure 5: Просмотр информации

Создание html-файла

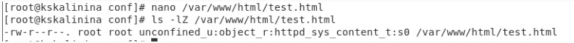


```
  GNU nano 2.3.1                          Файл: /var/www/html/test.html

<html>
<body>test</body>
</html>
```

Figure 6: Создание html-файла

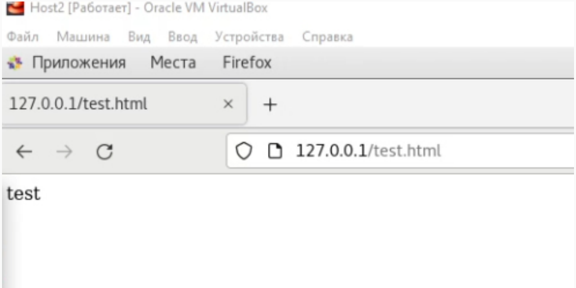
Контекст созданного файла



```
[root@kskalinina conf]# nano /var/www/html/test.html
[root@kskalinina conf]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Figure 7: Контекст html-файла, заданный по умолчанию

Обращение к файлу через веб-сервер

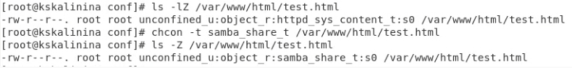


Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Firefox
127.0.0.1/test.html
127.0.0.1/test.html

test

Figure 8: Успешное чтение файла через веб-сервер

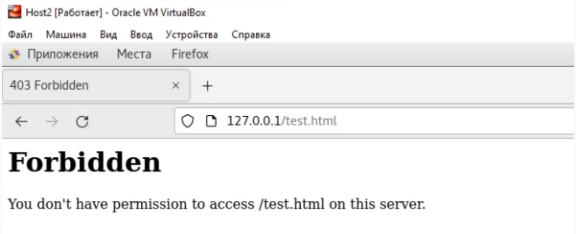
Изменение контекста файла с httpd_sys_content_t на samba_share_t



```
[root@kskalinina conf]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kskalinina conf]# chcon -t samba_share_t /var/www/html/test.html
[root@kskalinina conf]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 9: Изменение контекста html-файла

Повторная попытка доступа к файлу через веб-сервер

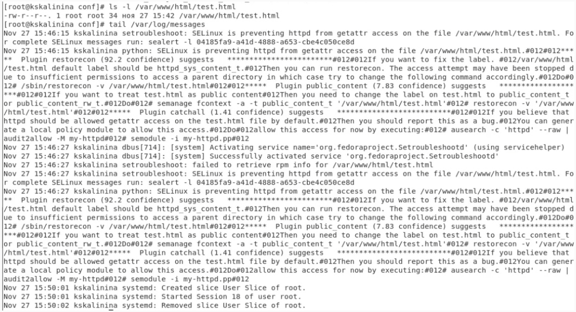

Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Firefox
403 Forbidden
127.0.0.1/test.html

Forbidden

You don't have permission to access /test.html on this server.

Figure 10: Ошибка доступа к файлу

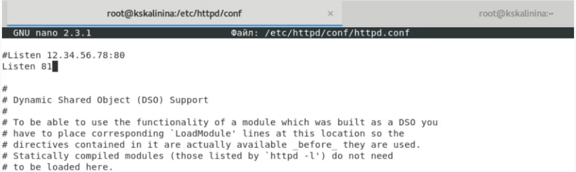
Просмотр прав файла и системного лог-файла



```
[root@kskalinina conf]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 ноя 27 15:42 /var/www/html/test.html
[root@kskalinina conf]# tail /var/log/messages
Nov 27 15:46:15 kskalinina setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. Fo
r complete SELinux messages run: sealert -l 04185fa9-a41d-4888-a653-cbe4c050ce8d
Nov 27 15:46:15 kskalinina python: SELinux is preventing httpd from getattr 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 d
ue to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /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 getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can gener
ate 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 -i my-httpd.pp#012
Nov 27 15:46:27 kskalinina dbus[714]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Nov 27 15:46:27 kskalinina dbus[714]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Nov 27 15:46:27 kskalinina setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Nov 27 15:46:27 kskalinina setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. Fo
r complete SELinux messages run: sealert -l 04185fa9-a41d-4888-a653-cbe4c050ce8d
Nov 27 15:46:27 kskalinina python: SELinux is preventing httpd from getattr 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 d
ue to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#0
12# /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 getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can gener
ate 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 -i my-httpd.pp#012
Nov 27 15:50:01 kskalinina systemd: Created slice User Slice of root.
Nov 27 15:50:01 kskalinina systemd: Started Session 18 of user root.
Nov 27 15:50:02 kskalinina systemd: Removed slice User Slice of root.
```

Figure 11: Просмотр прав файла и системного лог-файла

Запуск веб-сервер Apache на прослушивание TCP-порта 81



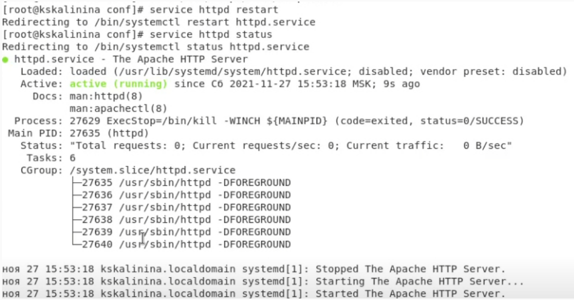
```
  GNU nano 2.3.1                        Файл: /etc/httpd/conf/httpd.conf

#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.
```

Figure 12: Смена TCP-порта

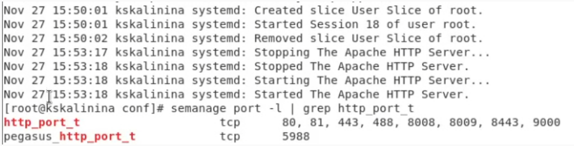
Перезапуск веб-сервера Apache и просмотр портов



```
[root@kskalinina conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@kskalinina conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Сб 2021-11-27 15:53:18 MSK; 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 27629 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 27635 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─27635 /usr/sbin/httpd -DFOREGROUND
           ├─27636 /usr/sbin/httpd -DFOREGROUND
           ├─27637 /usr/sbin/httpd -DFOREGROUND
           ├─27638 /usr/sbin/httpd -DFOREGROUND
           ├─27639 /usr/sbin/httpd -DFOREGROUND
           └─27640 /usr/sbin/httpd -DFOREGROUND

ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 15:53:18 kskalinina.localdomain systemd[1]: Started The Apache HTTP Server.
```

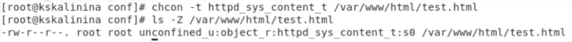
Figure 13: Перезапуск Apache



```
Nov 27 15:50:01 kskalinina systemd: Created slice User Slice of root.
Nov 27 15:50:01 kskalinina systemd: Started Session 18 of user root.
Nov 27 15:50:02 kskalinina systemd: Removed slice User Slice of root.
Nov 27 15:53:17 kskalinina systemd: Stopping The Apache HTTP Server...
Nov 27 15:53:18 kskalinina systemd: Stopped The Apache HTTP Server.
Nov 27 15:53:18 kskalinina systemd: Starting The Apache HTTP Server...
Nov 27 15:53:18 kskalinina systemd: Started The Apache HTTP Server.
[root@kskalinina 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
```

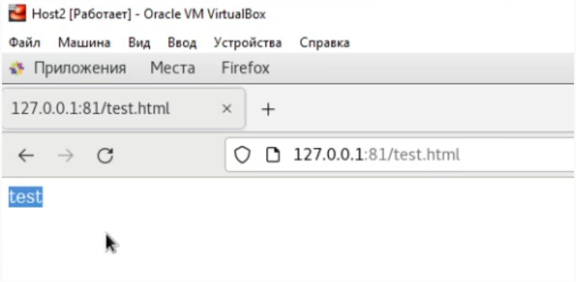
Figure 14: Просмотр списка портов

Возврат контекста httpd_sys_content__t файлу



```
[root@kskalinina conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kskalinina conf]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Figure 15: Смена контекста файла

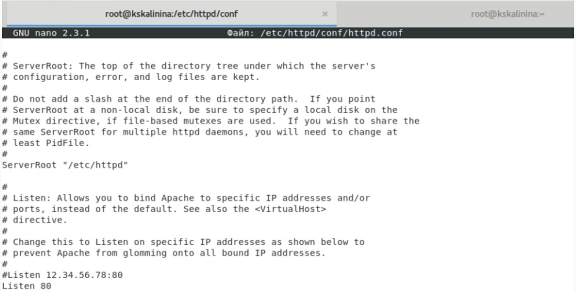


Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Firefox
127.0.0.1:81/test.html
127.0.0.1:81/test.html

test

Figure 16: Просмотр файла через 81 порт

Возвращение начального вида конфигурационного файла apache



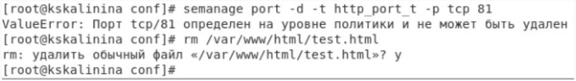
```
  GNU nano 2.3.1                    Файл: /etc/httpd/conf/httpd.conf

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Figure 17: Восстановление файла

Попытка удалить привязку http_port_t к 81 порту и удаление созданного файла



```
[root@kskalinina conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@kskalinina conf]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@kskalinina conf]#
```

Figure 18: Попытка удаления привязки http_port_t к 81 порту и удаление файла

Выводы

Выводы

Таким образом я успешно познакомилась с технологией SELinux и проверила работу SELinx на практике совместно с веб-сервером Apache.