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 лабораторной работы

Первым делом был осуществлён вход в систему и проверены режим и политика SELinux (Рис. 1)

```
[dnbabkov@dnbabkov ~]$ getenforce
Enforcing
[dnbabkov@dnbabkov ~]$ 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
Max kernel policy version:      31
```

С помощью команды `service httpd status` была проверена работа веб-сервера. С помощью команды `service httpd start` веб-сервер был запущен (Рис. 2, 3)

```
[dnbabkov@dnbabkov ~]$ 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 prese
t: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
```

```
[dnbabkov@dnbabkov ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Командой `ps auxZ | grep httpd` веб-сервер был найден в списке процессов, а также был определён его контекст безопасности (unconfined_t) (Рис. 4)

```
[dnbabkov@dnbabkov ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       3008  0.0  0.2 224092  5012 ?
Ss   23:08   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     3011  0.0  0.1 226176  3092 ?
S    23:08   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     3012  0.0  0.1 226176  3092 ?
S    23:08   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     3013  0.0  0.1 226176  3092 ?
S    23:08   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     3014  0.0  0.1 226176  3092 ?
S    23:08   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     3015  0.0  0.1 226176  3092 ?
S    23:08   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dnbabkov 3240 0.0  0.0 112
812 980 pts/0 R+ 23:11   0:00 grep --color=auto httpd
```

Командой sestatus -b | grep httpd было просмотрено текущее состояние переключателей SELinux для Apache (Рис. 5)

```
[dnbabkov@dnbabkov ~]$ 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
```

Большая часть из них имеет статус `off`

Командой `ls -lZ /var/www` был определён тип файлов и поддиректорий в директории `www` (Рис. 6)

```
[dnbabkov@dnbabkov ~]$ 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
```

В директории находятся две поддиректории типа object_r

В поддиректории /var/www/html файлы отсутствуют, а создание файлов разрешено только root пользователю

От имени суперпользователя был создан файл test.html. Содержимое файла:

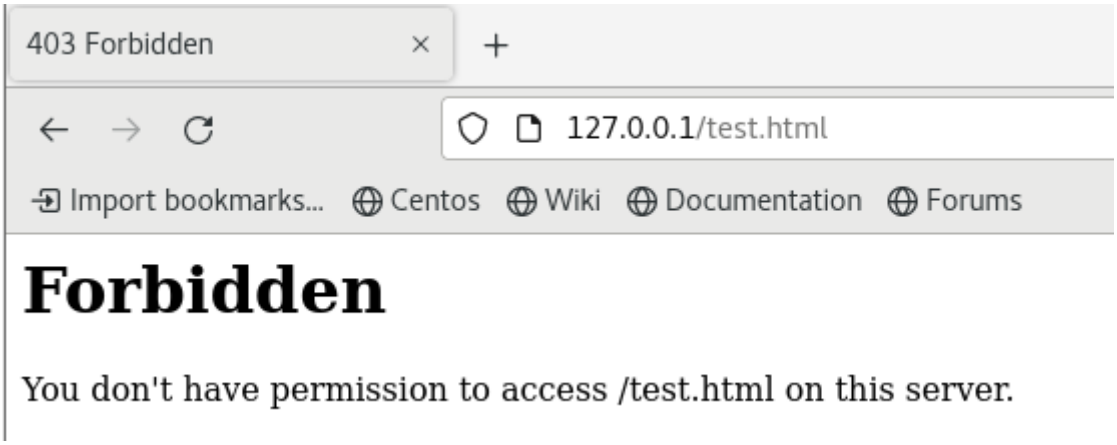
```
<html>
<body>test</body>
</html>
```

Далее к файлу было произведено обращение через веб-сервер (Рис. 7)

Следующим шагом контекст файла был изменён на `samba_share_t` (Рис. 8)

```
[root@dnbabkov html]# chcon -t samba_share_t /var/www/html/test.html
[root@dnbabkov html]# 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
```

При попытке получить доступ к файлу через веб-сервер была получена ошибка (Рис. 9)



Файл не был отображён, потому что параметры безопасности SELinux не позволяют веб-серверу открывать файлы, не являющиеся `httpd_sys_content_t`

Далее были просмотрены log-файлы веб-сервера Apache (Рис. 10)

```
[root@dnbabkov html]# tail /var/log/messages
Oct 11 23:23:04 dnbabkov dbus[715]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 11 23:23:04 dnbabkov dbus[715]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 11 23:23:04 dnbabkov setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 11 23:23:05 dnbabkov setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.
For complete SELinux messages run: sealert -l 974f588d-2d7e-40f4-a1b3-c1aa72dc7d80
Oct 11 23:23:05 dnbabkov 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/ww
w/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 accord
ingly.#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.htm
l to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#01
2# 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 repo
rt this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by execut
ing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Oct 11 23:23:16 dnbabkov dbus[715]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 11 23:23:17 dnbabkov dbus[715]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 11 23:23:17 dnbabkov setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 11 23:23:17 dnbabkov setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.
For complete SELinux messages run: sealert -l 974f588d-2d7e-40f4-a1b3-c1aa72dc7d80
Oct 11 23:23:17 dnbabkov 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/ww
w/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 accord
ingly.#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.htm
l to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#01
2# 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 repo
rt this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by execut
ing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
```

Далее в файле `/etc/httpd/httpd.conf` была найдена строчка Listen 80, и заменена на Listen 81

После перезапуска веб-сервера сбоя не произошло, потому что порт 81 тоже является частью политики Apache (Рис. 11)

```
[root@dnbabkov conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@dnbabkov conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@dnbabkov conf]# tail -nl /var/log/messages
tail: l: invalid number of lines
[root@dnbabkov conf]# tail -l /var/log/messages
Oct 11 23:29:34 dnbabkov systemd: Stopping The Apache HTTP Server...
Oct 11 23:29:35 dnbabkov systemd: Stopped The Apache HTTP Server.
Oct 11 23:29:35 dnbabkov systemd: Starting The Apache HTTP Server...
Oct 11 23:29:35 dnbabkov systemd: Started The Apache HTTP Server.
```

Далее была произведена попытка добавить порт 81, которая не удалась по причине того, что порт уже существует (Рис. 12)

```
[root@dnbabkov conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@dnbabkov conf]# semenage port -l | grep http_port_t
bash: semenage: command not found...
[root@dnbabkov 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
```

Если бы порта не было, то попытка перезапуска веб-сервера провалилась бы по причине того, что он не смог бы осуществить подключение. При добавлении порта подключение вновь стало бы возможно.

Следующим шагом файлу test.html был возвращен изначальный контекст, и произведено открытие файла в браузере (Рис. 13)

Конфигурационный файл Apache был возвращён в изначальное состояние. Была произведена попытка удалить порт 81 (Рис. 14)

```
[root@dnbabkov conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Последним шагом было удаление файла test.html