Лабораторная работа №6

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель

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

Задачи

1. Подготовить лабораторный стенд;
2. Запустить `Apache` в системе;
3. Создать небольшой веб-сервер;
4. Посмотреть различные варианты настроек сервера и изучить реакции на изменение этих настроек.

Выполнение лабораторной работы

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команды sestatus.

```
sestatus
```

```
[vemanaeva@vemanaeva ~]$ 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
```

Рис. 1: Проверим SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает

```
sudo systemctl start httpd
service httpd status
```

```
[vemanaeva@vemanaeva ~]$ sudo systemctl start httpd
[vemanaeva@vemanaeva ~]$ 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 2023-10-14 14:38:31 MSK; 2s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 3617 (httpd)
   Status: "Processing requests..."
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─3617 /usr/sbin/httpd -DFOREGROUND
           ├─3621 /usr/sbin/httpd -DFOREGROUND
           ├─3622 /usr/sbin/httpd -DFOREGROUND
           ├─3623 /usr/sbin/httpd -DFOREGROUND
           ├─3624 /usr/sbin/httpd -DFOREGROUND
           └─3625 /usr/sbin/httpd -DFOREGROUND

окт 14 14:38:31 vemanaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 14:38:31 vemanaeva.localdomain httpd[3617]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using vemanaeva.localdomain. Set the 'ServerName' dire... this message
окт 14 14:38:31 vemanaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[vemanaeva@vemanaeva ~]$
```

Рис. 2: Проверяем

Найдём веб-сервер Apache в списке процессов и определим его контекст безопасности

```
ps auxZ | grep httpd
ps -eZ | grep httpd
```

```
[vemanaeva@vemanaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3617  0.3  0.2 230444  5224 ?        Ss   14:38   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3621  0.0  0.1 232528  3160 ?        S    14:38   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3622  0.0  0.1 232528  3160 ?        S    14:38   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3623  0.0  0.1 232528  3160 ?        S    14:38   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3624  0.0  0.1 232528  3160 ?        S    14:38   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3625  0.0  0.1 232528  3160 ?        S    14:38   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vemanae+ 3661 0.0  0.0 112832 972 pts/0 R+ 14:38   0:00 grep --color=auto httpd
[vemanaeva@vemanaeva ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0     3617 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3621 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3622 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3623 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3624 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0     3625 ?        00:00:00 httpd
```

Рис. 3: Контекст безопасности

Посмотрим текущее состояние переключателей SELinux для Apache

sestatus -bigrep httpd

```
[vemanaeva@vemanaeva ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
cluster_can_network_connect                 off
cluster_manage_all_files                    off
cluster_use_execmem                         off
cobbler_anon_write                          off
cobbler_can_network_connect                 off
cobbler_use_cifs                            off
cobbler_use_nfs                             off
collectd_tcp_network_connect                off
condor_tcp_network_connect                  off
conman_can_network                          off
conman_use_nfs                              off
container_connect_any                       off
cron_can_relabel                            off
cron_system_cronjob_use_shares              off
cron_userdomain_transition                  on
cups_execmem                                off
cvs_read_shadow                             off
daemons_dump_core                           off
daemons_enable_cluster_mode                 off
daemons_use_tcp_wrapper                     off
daemons_use_tty                             off
```

Определим тип файлов и поддиректорий, находящихся в директории /var/www

```
ls -lZ /var/www
```

```
[vemanaeva@vemanaeva ~]$ 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
[vemanaeva@vemanaeva ~]$
```

Рис. 5: Типы поддиректорий и файлов в директории /var/www

Определим тип файлов, находящихся в директории /var/www/html

```
ls -lZ /var/www/html
```

```
[vemanaeva@vemanaeva ~]$ ls -lZ /var/www/html
[vemanaeva@vemanaeva ~]$
```

Рис. 6: Тип файлов в директории /var/www/html

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html (только суперпользователь)

```
ls -l /var/www
```

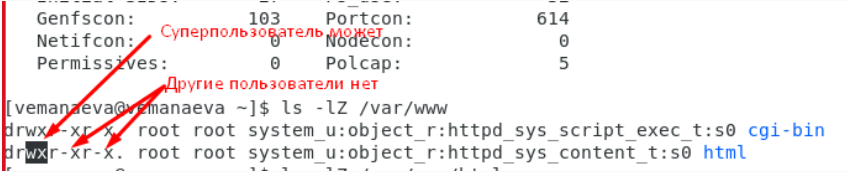
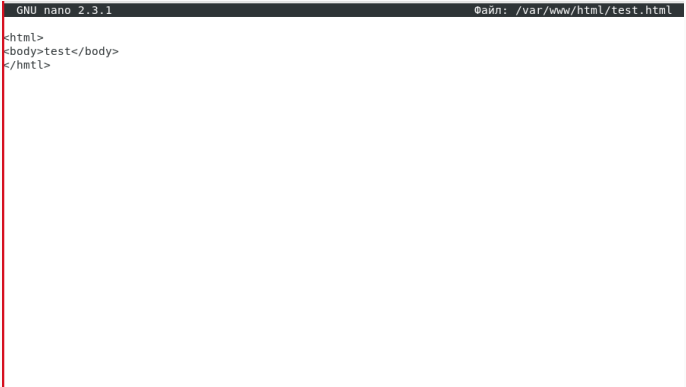


Рис. 7: Определим права на файл

Создадим от имени суперпользователя html-файл /var/www/html/test.html

```
sudo nano /var/www/html/test.html

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



Проверим контекст созданного файла.

```
ls -Z /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ 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
```

Рис. 9: Определим контекст

Обратимся к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Убедимся, что файл был успешно отображён.

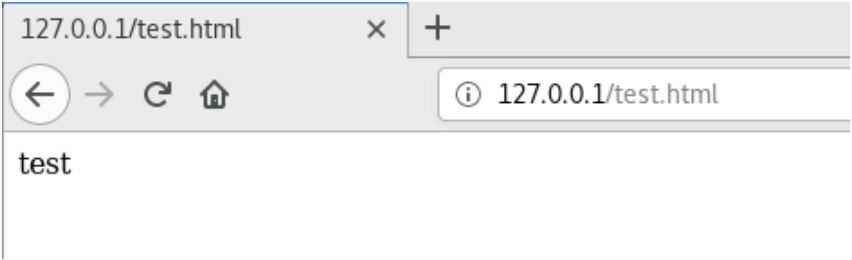


Рис. 10: http://127.0.0.1/test.html

Измените контекст файла `/var/www/html/test.html` с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа

```
sudo chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[vemanaeva@vemanaeva ~]$ 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
[vemanaeva@vemanaeva ~]$
```

Рис. 11: Изменяем контекст файла

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. И получаем сообщение об ошибке Forbidden.

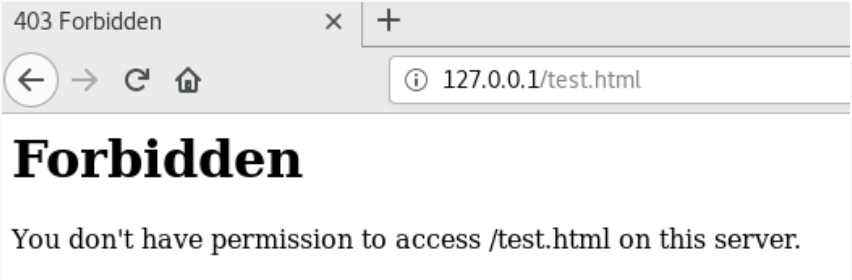


Рис. 12: http://127.0.0.1/test.html

Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache.

```
ls -l /var/www/html/test.html
tail /var/log/messages
```

```
[vemanaeva@vemanaeva ~]$ sudo tail /var/log/messages
Oct 14 14:54:03 vemanaeva dbus[703]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 14:54:04 vemanaeva dbus[703]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 14:54:04 vemanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 14:54:04 vemanaeva setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 9855aefb-a7c6-4206-bcd5-73265f5aa3be
Oct 14 14:54:04 vemanaeva 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#01
2If 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 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 -i my-httpd.pp#012
Oct 14 14:54:16 vemanaeva dbus[703]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 14:54:17 vemanaeva dbus[703]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 14:54:17 vemanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 14:54:17 vemanaeva setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 9855aefb-a7c6-4206-bcd5-73265f5aa3be
Oct 14 14:54:17 vemanaeva 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#01
2If 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 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 -i my-httpd.pp#012
[vemanaeva@vemanaeva ~]$
```

Рис. 13: log-файлы

Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов. Убедимся, что порт 81 появился в списке.

```
sudo semanage port -a -t http_port_t --proto tcp 81
semanage port -l | grep http_port_t
```

```
[vemanaeva@vemanaeva ~]$ sudo semanage port -a -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 уже определен
[vemanaeva@vemanaeva ~]$ ^C
[vemanaeva@vemanaeva ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[vemanaeva@vemanaeva ~]$ sudo 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
```

Рис. 14: Список портов

Вернём контекст `httpd_sys_content__t` к файлу `/var/www/html/test.html`.

После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.

```
chcon -t httpd_sys_content_t /var/www/html/test.html
```

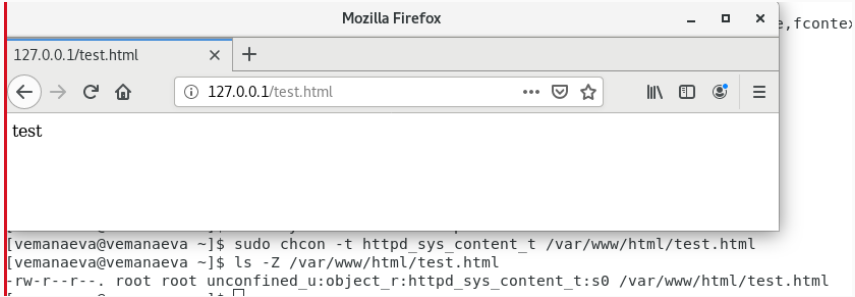


Рис. 15: http://127.0.0.1:81/test.html

Выводы по проделанной работе

Вывод

В результате выполнения работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinx на практике совместно с веб-сервером Apache.

Были записаны скринкасты выполнения и защиты лабораторной работы.