Ощепков Дмитрий Владимирович НКАбд-02-22

Дисциплина: Основы информационной безопасности

Лабораторная работа №6

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

Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus

```
Выполнено!
[dvothepkov@localhost ~]$ getenforce
Enforcing
[dvothepkov@localhost ~]$ sestatus
SELinux status:
                                       enabled
SELinuxfs mount:
                                      /sys/fs/selinux
SELinux root directory:
Loaded policy name:
                                      /etc/selinux
                                      targeted
Mode from config file: enforcing
Policy MLS status:
Policý deny_unknown status: allowed
Memory protection checking: actual (
Max kernel policy version: 33
                                       actual (secure)
[dvothepkov@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
```

Обратился с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

[dvothepkov@localhost ~]\$ service httpd status

```
[v1132226428@1132226428 ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service

* httpd.service - The Apache HTTP Server
Loaded: loaded (Jusr/lib/system/system/httpd.service; enabled; preset: dip
Active: active (running) since Fri 2024-04-26 17:12:51 MSK; 7min ago
Docs: man:httpd.service(8)
Main PTD: 125239 (httpd)
Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes
Tasks: 213 (limit: 4460)
Memory: 19.7M
CPU: 336ms
CGroup: /system.slice/httpd.service
- 125239 /usr/sbin/httpd -DFOREGROUND
- 125244 /usr/sbin/httpd -DFOREGROUND
- 125244 /usr/sbin/httpd -DFOREGROUND
- 125245 /usr/sbin/httpd -DFOREGROUND
- 125246 /usr/sbin/httpd -DFOREGROUND
- 125245 /usr/sbin/httpd -DFOREGROUND
- 125246 /usr/sbin/httpd -DFOREGROUND
- 125246 /usr/sbin/httpd -DFOREGROUND
- 125245 /usr/sbin/httpd -DFOREGROUND
- 125245 /usr/sbin/httpd -DFOREGROUND
- 125245 /usr/sbin/httpd -DFOREGROUND
- 125246 /usr/sbin/httpd -
```

Найшел веб-сервер Apache в списке процессов, определил его контекст безопасности и занес эту информацию в отчёт.

```
₽Ŧ.
                            dvothepkov@localhost:~
                                                              Q
                                                                   ≡
  dvothepkov@localhost:~ — /bin/s... ×
                                           dvothepkov@localhost:~
[dvothepkov@localhost ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dvothep+ 42134 0.0
236232 8920 pts/0 S+ 18:02    0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 dvothep+ 42182 0.0 0.0
[dvothepkov@localhost ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'
Usage: sestatus [OPTION]

    -v Verbose check of process and file contexts.

 -b Display current state of booleans.
Without options, show SELinux status.
[dvothepkov@localhost ~]$ seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/v] v
* Waiting in queue...
The following packages have to be installed:
```

Определил тип файлов и поддиректорий, находящихся в директории

```
[dvothepkov@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28
12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28
12:35 html
```

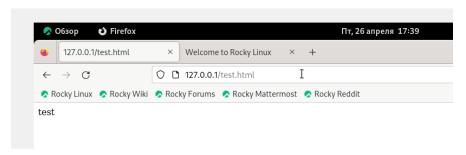
Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

```
[root@1132226428 v1132226428]# touch /var/www/html/test.html
[root@1132226428 v1132226428]# nano /var/www/html/test.html
[root@1132226428 v1132226428]# cat /var/www/html/test.html
<html
<html>
<hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor="block"><hcolor=
```

Проверил контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html

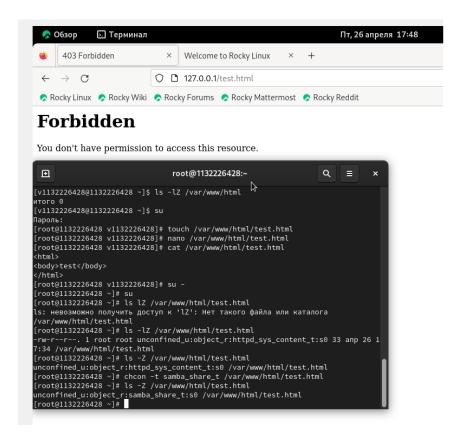
```
[root@1132226428 ~]# ls -lZ /var/www/html/test.html
-rw-r--r-. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 anp 26 1
7:34 /var/www/html/test.html
[root@1132226428 ~]#
```

Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён



Изменил контекст файла /var/www/html/test.html c 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 проверил, что контекст поменялся. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.



Просмотрел log-файлы веб-сервера Арасhe. Также просмотрел системный лог-файл:

Попробовал 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 нашел строчку Listen 80 и заменил её на Listen 81.

```
root@1132226428:-

Q = X

GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Изменён
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.

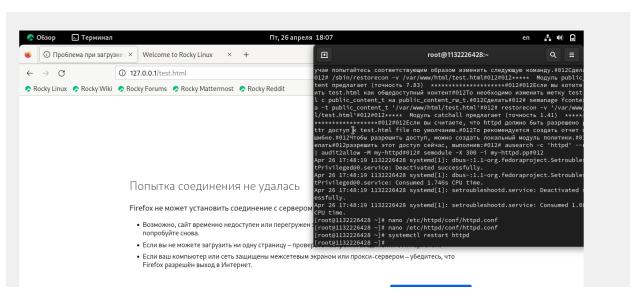
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the 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

AG Cnpaвкa AO Записать AW Поиск AK Вырезать AT Выполнить AC Позиция
AX Выход AR Читфайл AN Замена AU Вставить AD Выровнять A K строке
```

Выполнил перезапуск веб-сервера Apache



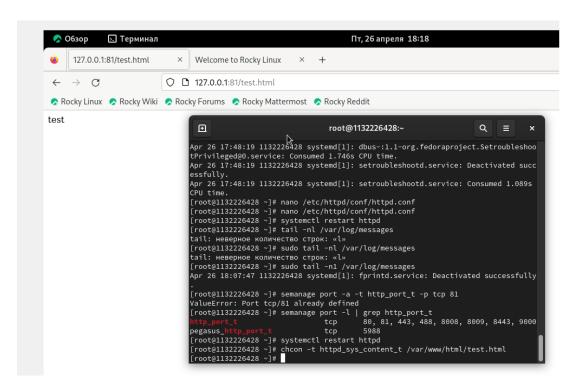
Проанализировал лог-файлы

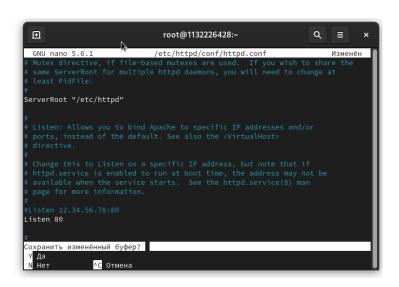
```
tail: неверное количество строк: «l»
[root@1132226428 ~]# sudo tail -n1 /var/log/messages
Apr 26 18:07:47 1132226428 systemd[1]: fprintd.service: Deactivated successfully
.
[root@1132226428 ~l# s
```

Выполнил следующую команду

```
[root@1132226428 ~] # semanage port -a -t http_port_t -p tcp 81

ValueError: Port tcp/81 already defined
[root@1132226428 ~] # 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
[root@1132226428 ~] # systemctl restart httpd
[root@1132226428 ~] #
```





Удалил привязку http_port_t к 81 порту

[root@1132220428 ~]# semanage port -d -t http_port_t -p tcp 81

Удалил файл

valuetrror: Port tcp/81 is detined in policy, cannot be deleted [root@1132226428 ~]# rm /var/www/html/test.html rm: удалить обычный файл '/var/www/html/test.html'? у [root@1132226428 ~]#

Вывод: развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.