Ощепков Дмитрий Владимирович НКАбд-02-22

Дисциплина: Основы информационной безопасности

Лабораторная работа №6

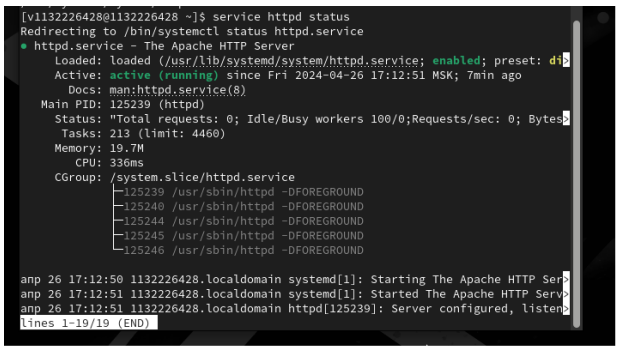
Цель работы: развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

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

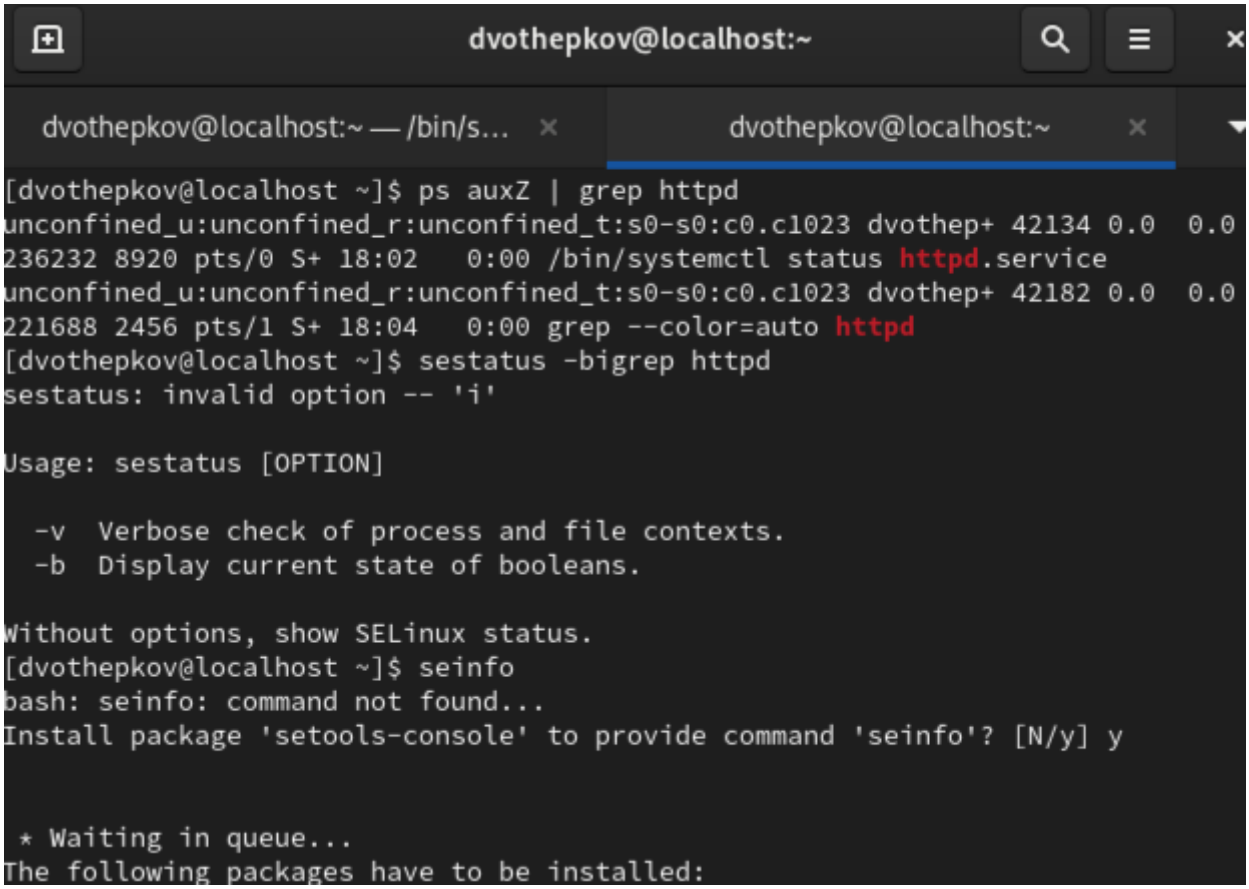
```
Выполнено!
[dvothepkov@localhost ~]$ getenforce
Enforcing
[dvothepkov@localhost ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   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
[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:

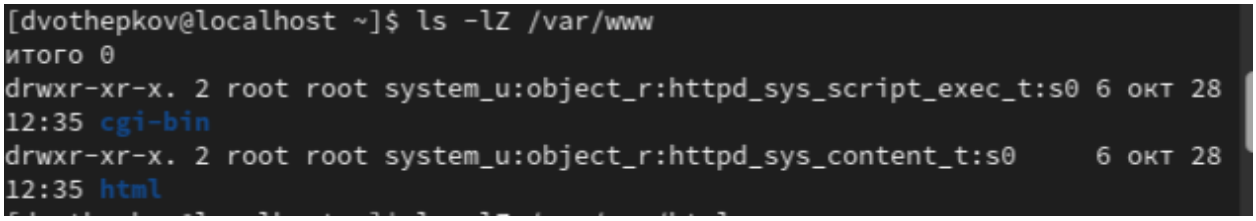
```
[dvothepkov@localhost ~]$ service httpd status
```



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

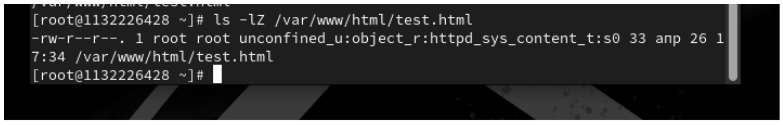


Определил тип файлов и поддиректорий, находящихся в директории

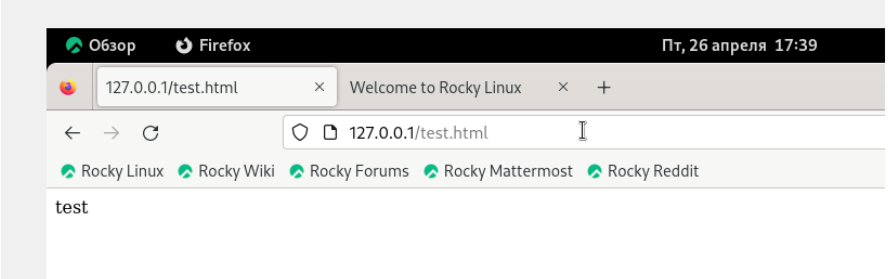


Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

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

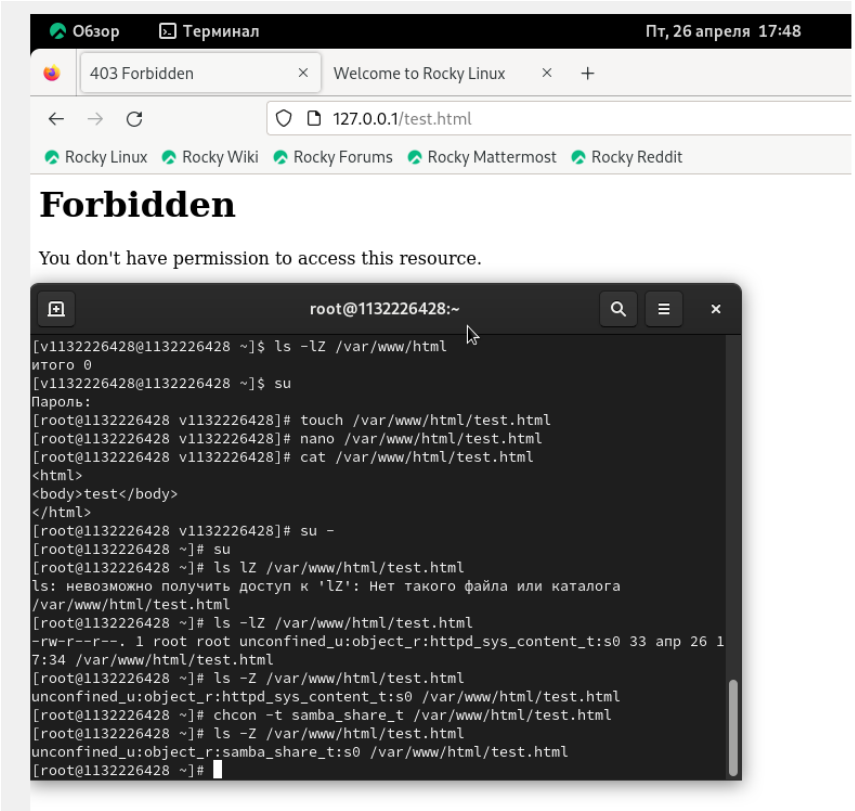


Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён

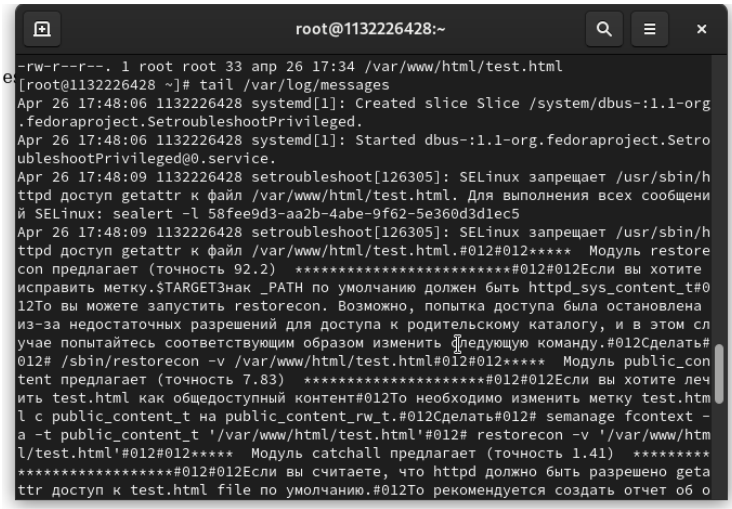


Изменил контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html

После этого 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.

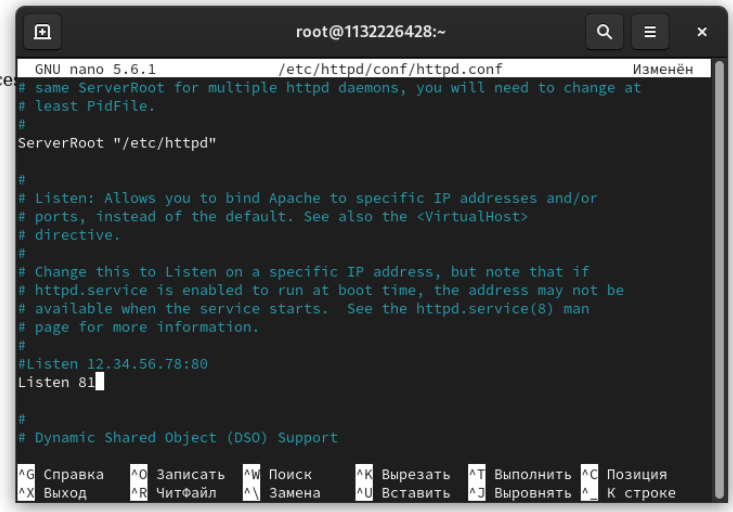


Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл:

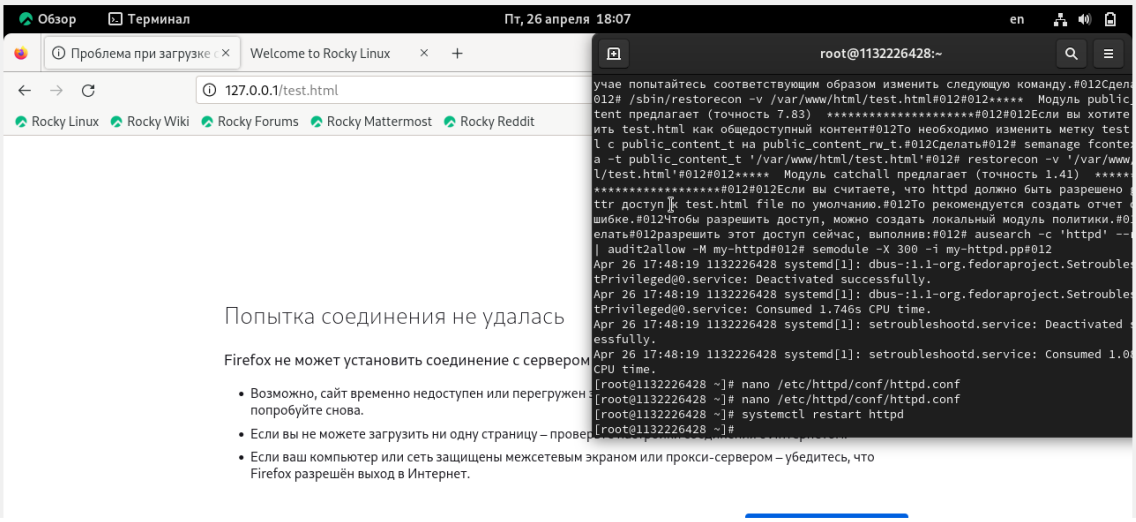


Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашел строчку Listen 80 и заменил её на Listen 81.

acce



Выполнил перезапуск веб-сервера Apache

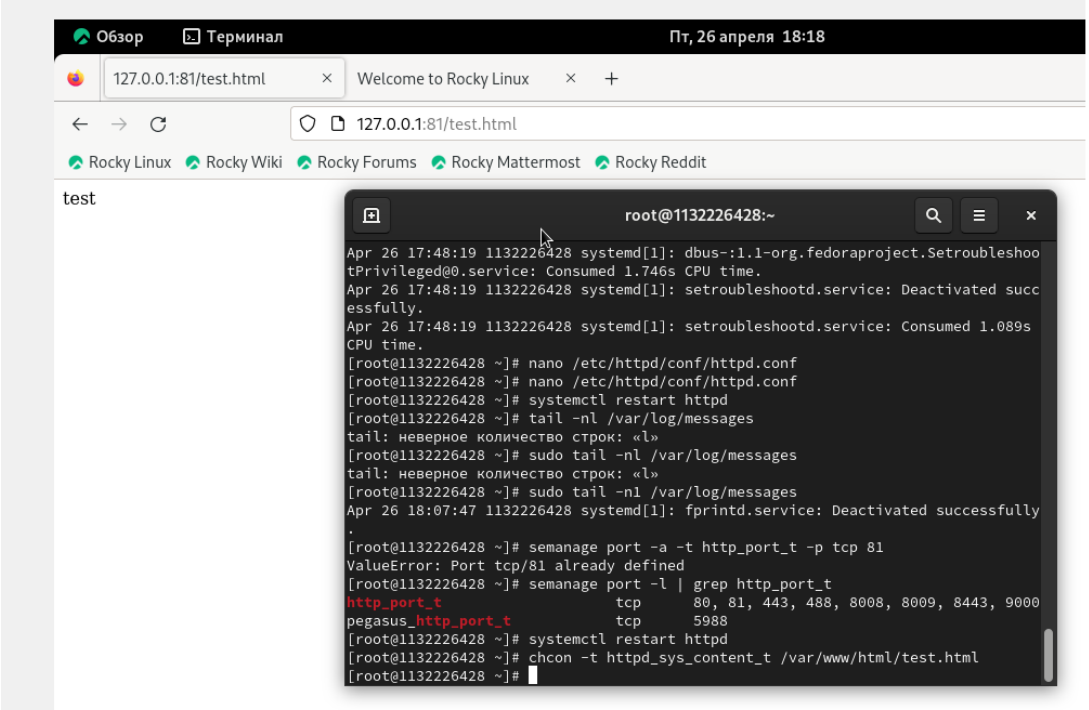


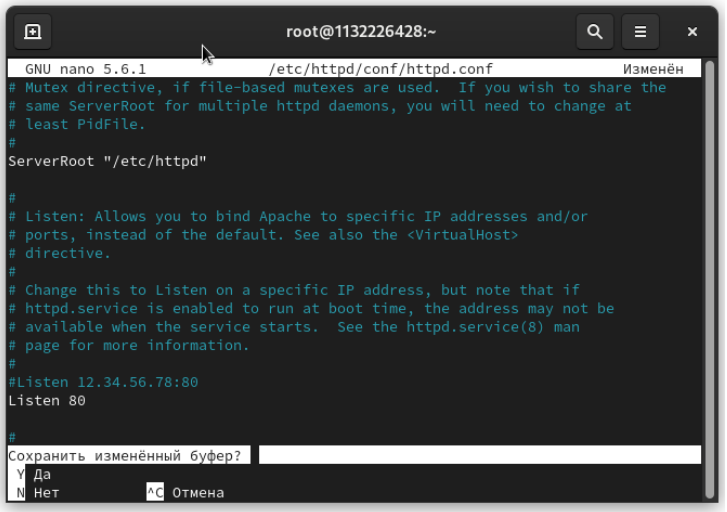
Проанализировал лог-файлы

```
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 ~]# 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 ~]#
```


Обзор
Терминал
Пт, 26 апреля 18:18
127.0.0.1:81/test.html
Welcome to Rocky Linux
127.0.0.1:81/test.html
Rocky Linux
Rocky Wiki
Rocky Forums
Rocky Mattermost
Rocky Reddit
test
root@1132226428:~
Apr 26 17:48:19 1132226428 systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.746s CPU time.
Apr 26 17:48:19 1132226428 systemd[1]: setroubleshootd.service: Deactivated successfully.
Apr 26 17:48:19 1132226428 systemd[1]: setroubleshootd.service: Consumed 1.089s CPU time.
[root@1132226428 ~]# nano /etc/httpd/conf/httpd.conf
[root@1132226428 ~]# nano /etc/httpd/conf/httpd.conf
[root@1132226428 ~]# systemctl restart httpd
[root@1132226428 ~]# tail -nl /var/log/messages
tail: неверное количество строк: «l»
[root@1132226428 ~]# sudo tail -nl /var/log/messages
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 ~]# 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 ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@1132226428 ~]#


root@1132226428:~
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Изменён
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 80
#
Сохранить изменённый буфер?
Y Да
N Нет
^C Отмена

Удалил привязку http_port_t к 81 порту

Удалил файл

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