Защита лабораторной работы №6 Мандатное разграничение прав в Linux

Исаханян Эдуард Тигранович

2022 Sep 21th

RUDN University, Moscow, Russian Federation

Защита лабораторной работы №6

Цель

Цель

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Подготовка лабораторного стенда

Параметр ServerName

```
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
```

Figure 1: Параметр ServerName

Отключение фильтра

```
[root@edikisakhayan conf]# iptables -P INPUT ACCEPT
[root@edikisakhayan conf]# iptables -F
[root@edikisakhayan conf]# iptables -P OUTPUT ACCEPT
```

Figure 2: Отключение фильтра

Отключение фильтра

```
[root@edikisakhayan conf]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@edikisakhayan conf]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@edikisakhayan conf]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@edikisakhayan conf]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

Figure 3: Отключение фильтра

Выполнение лабораторной работы

Проверка режима и политики

```
[root@edikisakhayan conf]# getenforce
Enforcing
[root@edikisakhayan conf]# 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
```

Figure 4: Проверка режима и политики

Проверка через браузер

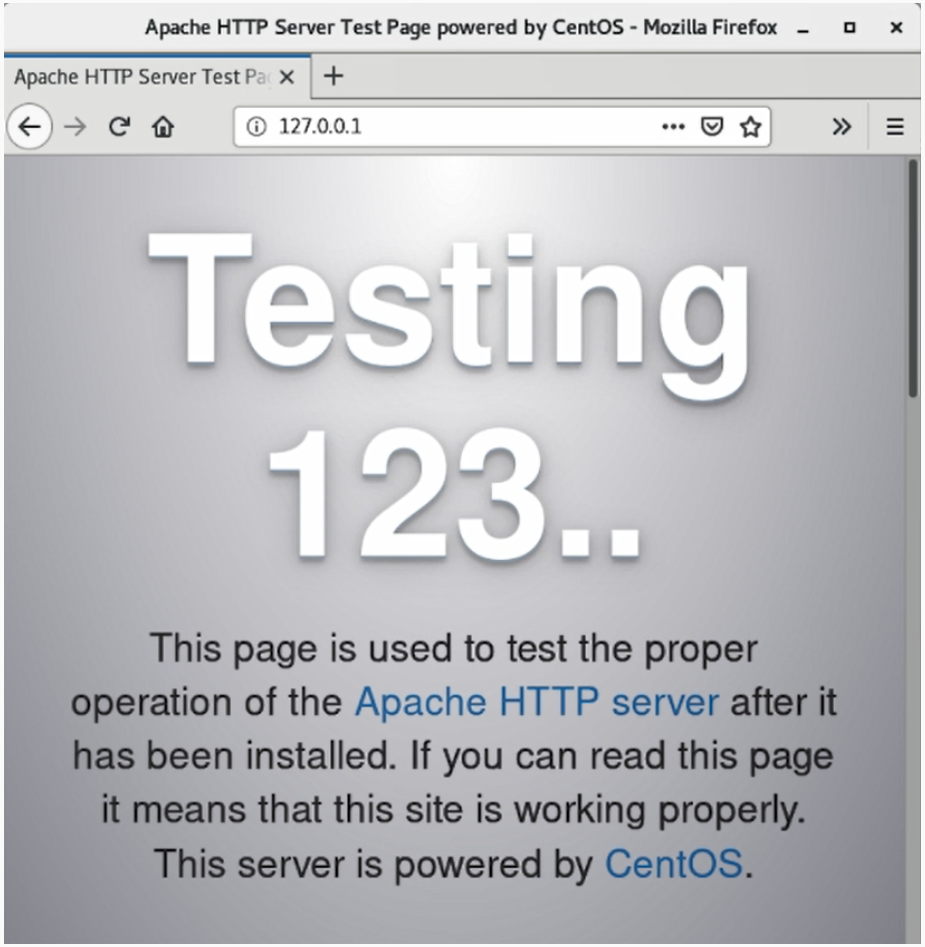


Figure 5: Проверка через браузер

Проверка через браузер

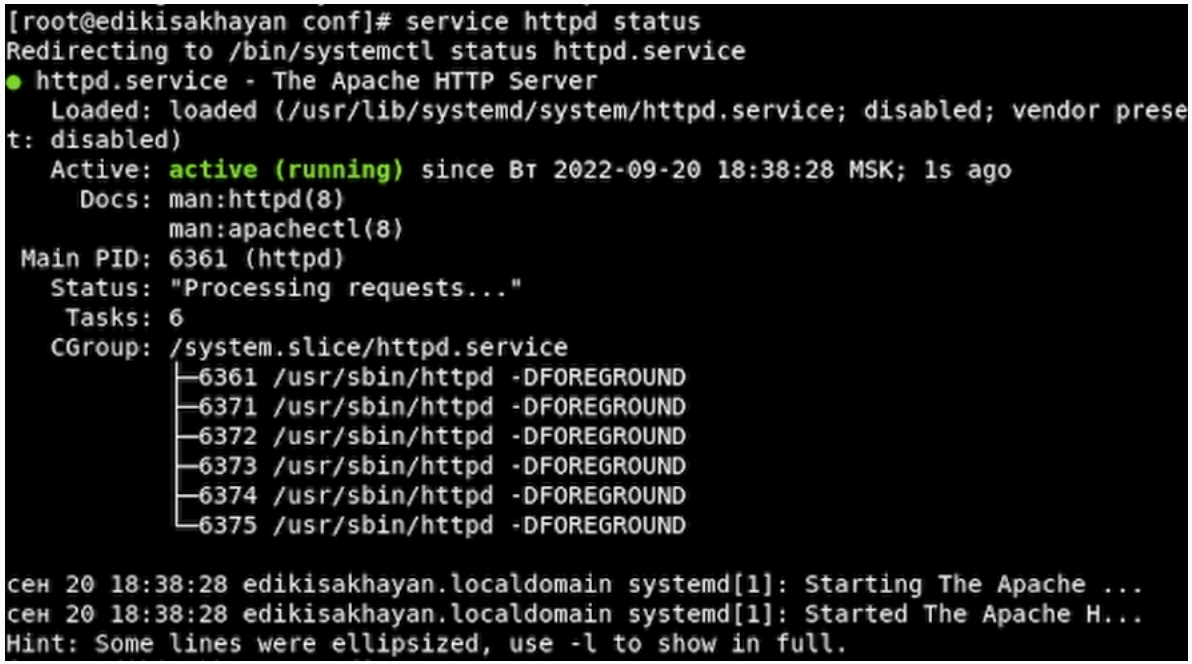


Figure 6: Проверка статуса

веб-сервер Apache

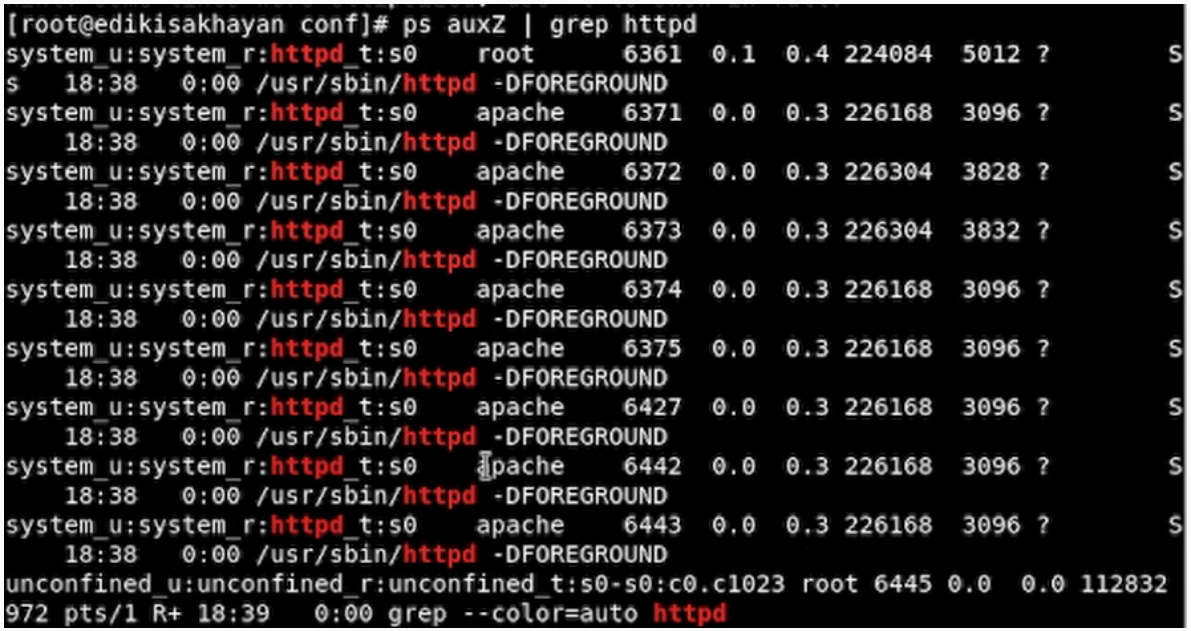


Figure 7: веб-сервер Apache

Просмотр переключателей SELinux для Apache

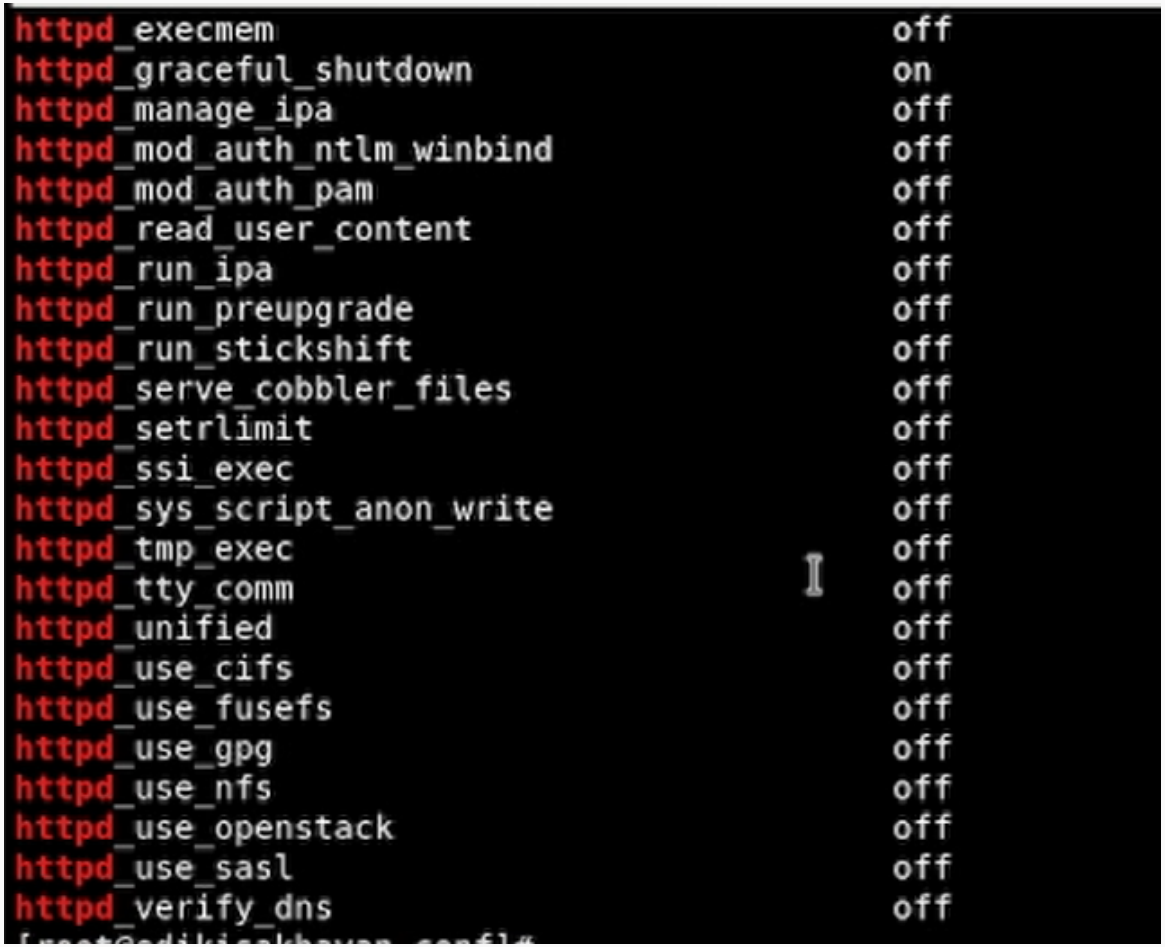
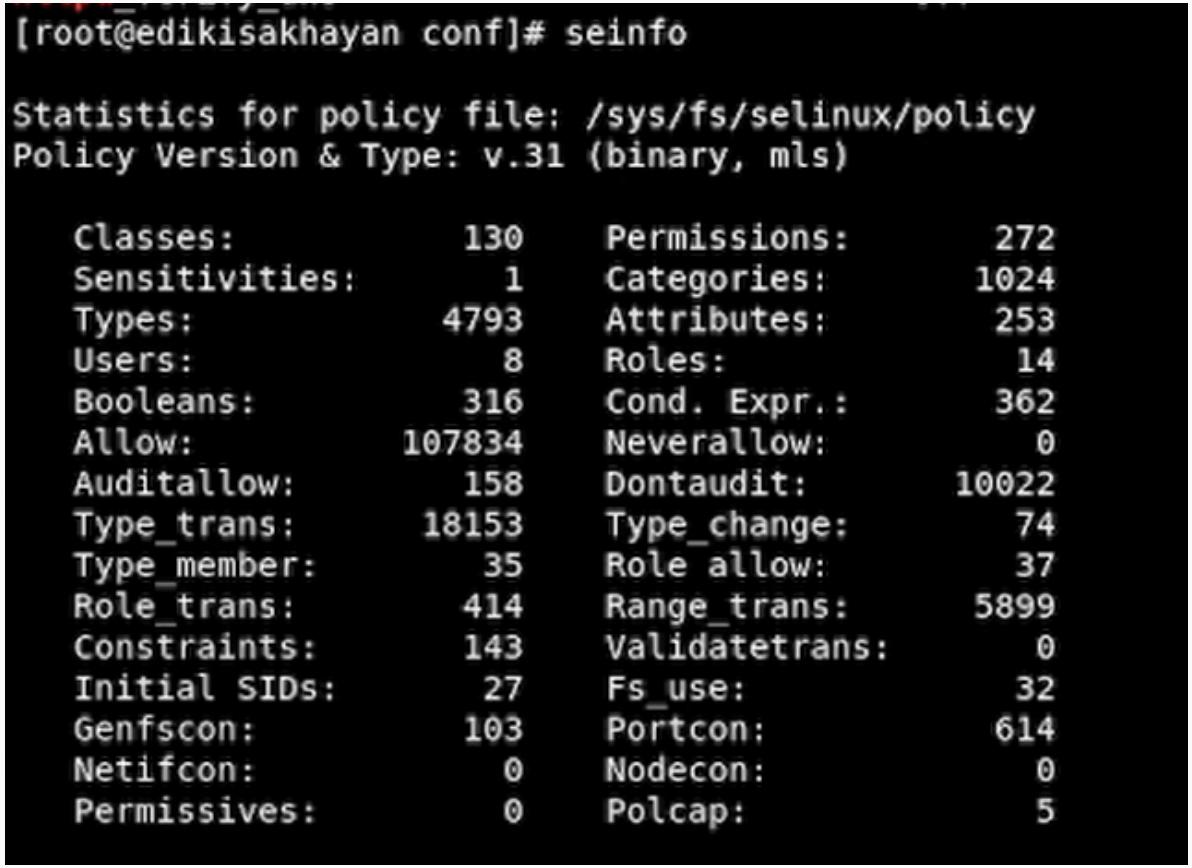


Figure 8: Просмотр переключателей SELinux для Apache

Статистика



```
[root@edikisakhayan 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 9: Статистика

Определение типов файлов и круг пользователей

```
[root@edikisakhayan 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@edikisakhayan conf]# ls -lZ /var/www/html/
[root@edikisakhayan conf]# ls -l /var/www/html/
итого 0
[root@edikisakhayan conf]# ls -l /var/www/
итого 0
drwxr-xr-x. 2 root root 6 мар 24 17:58 cgi-bin
drwxr-xr-x. 2 root root 6 мар 24 17:58 html
```

Figure 10: Определение типов файлов и круг пользователей

Создание файла

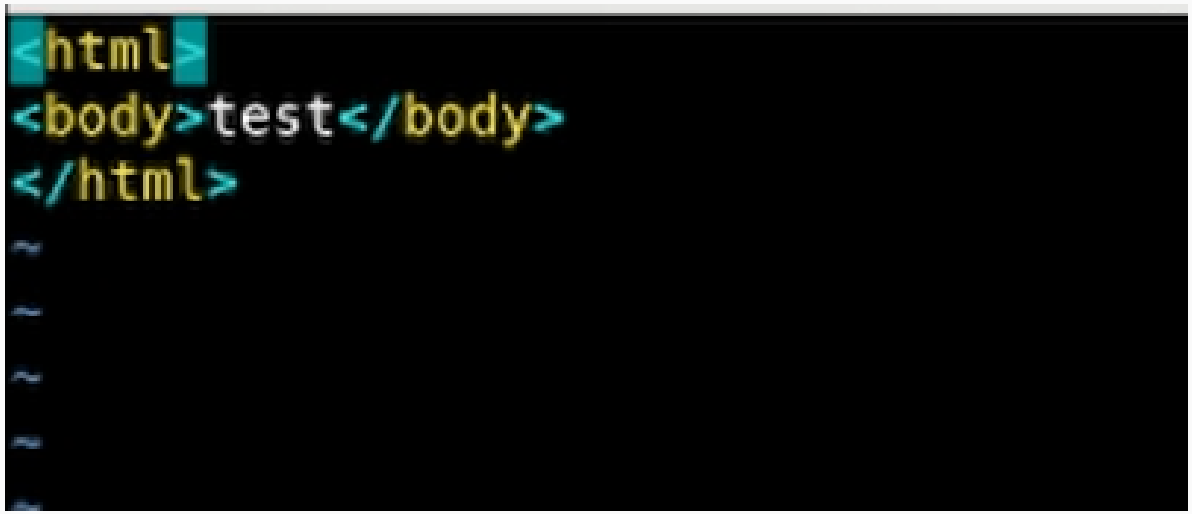


Figure 11: Создание файла

Проверка

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

Figure 12: Проверка

Получение доступа к файлу через браузер

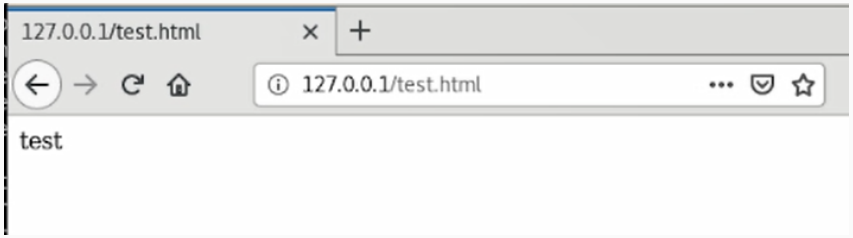


Figure 13: Получение доступа к файлу через браузер

Изменение контекста, проверка

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

Figure 14: Изменение контекста, проверка

Получение доступа к файлу через браузер

Figure 15: Получение доступа к файлу через браузер

Анализ ситуации

Figure 16: Анализ ситуации

Изменеие порта 80 на 81

```
#
# 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 81

#
```

Figure 17: Изменеие порта 80 на 81

Анализ и просмотр лог-файлов

Figure 18: Анализ и просмотр лог-файлов

Выполнение и проверка

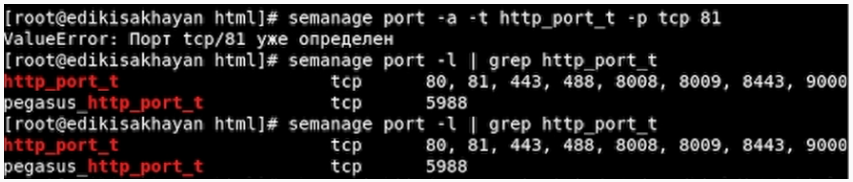


Figure 19: Выполнение и проверка

Возвращение контекста

```
[root@edikisakhayan html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@edikisakhayan html]#
```

Figure 20: Возвращение контекста

Получение доступа к файлу через браузер

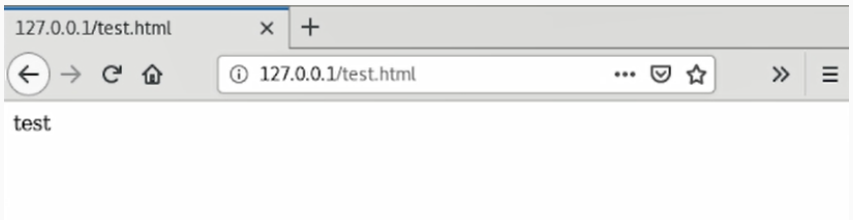


Figure 21: Получение доступа к файлу через браузер

Исправленный файл apache

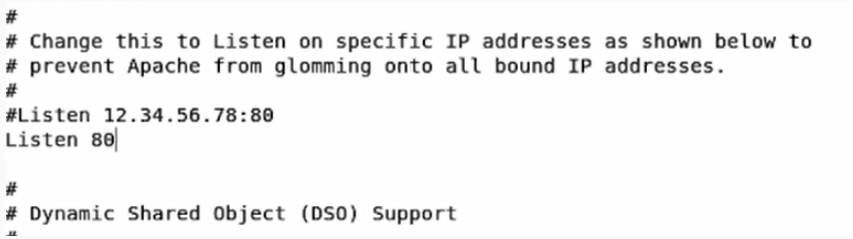


Figure 22: Исправленный файл apache

Удаление привязки к 81 порту и удаление файла

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

Figure 23: Удаление привязки к 81 порту и удаление файла

Вывод

Вывод

Входе работы, мы развили навыки администрирования ОС Linux.

Получили первое практическое знакомство с технологией SELinux.

Проверили работу SELinx на практике совместно с веб-сервером Apache.