

Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Исаханян Эдуард Тигранович

2022 Sep 21th

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Подготовка лабораторного стенда	6
2.2	Выполнение лабораторной работы	7
3	Выводы	15
	Список литературы	16

List of Tables

List of Figures

2.1	Параметр ServerName	6
2.2	Отключение фильтра	6
2.3	Отключение фильтра	6
2.4	Проверка режима и политики	7
2.5	Проверка через браузер	8
2.6	Проверка статуса	8
2.7	веб-сервер Apache	9
2.8	Просмотр переключателей SELinux для Apache	9
2.9	Статистика	10
2.10	Определение типов файлов и круг пользователей	10
2.11	Создание файла	11
2.12	Проверка	11
2.13	Получение доступа к файлу через браузер	11
2.14	Изменение контекста, проверка	11
2.15	Получение доступа к файлу через браузер	12
2.16	Анализ ситуации	12
2.17	Изменеие порта 80 на 81	12
2.18	Анализ и просмотр лог-файлов	13
2.19	Выполнение и проверка	13
2.20	Возвращение контекста	13
2.21	Получение доступа к файлу через браузер	13
2.22	Исправленный файл apache	13
2.23	Удаление привязки к 81 порту и удаление файла	14

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Подготовка лабораторного стенда

В конфигурационном файле /etc/httpd/httpd.conf зададим параметр ServerName.
(рис. 2.1)

```
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 2.1: Параметр ServerName

Также проследим, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключим фильтр и добавим разрешающие правила. (рис. 2.2 - 2.3)

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

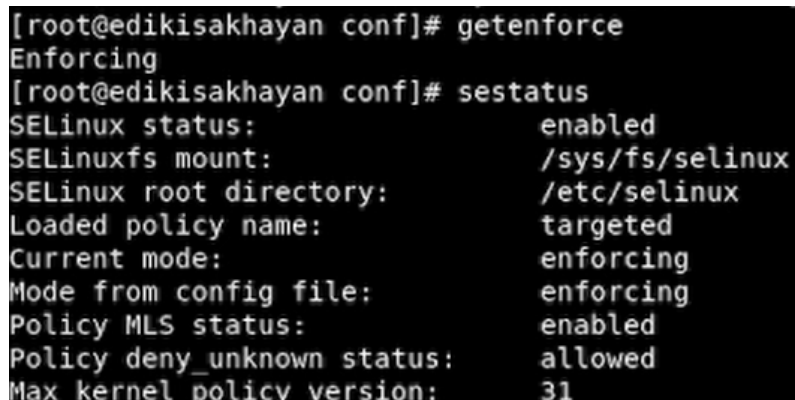
Figure 2.2: Отключение фильтра

```
[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 2.3: Отключение фильтра

2.2 Выполнение лабораторной работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted. (рис. 2.4)



```
[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 2.4: Проверка режима и политики

Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает. (рис. 2.5 - 2.6)

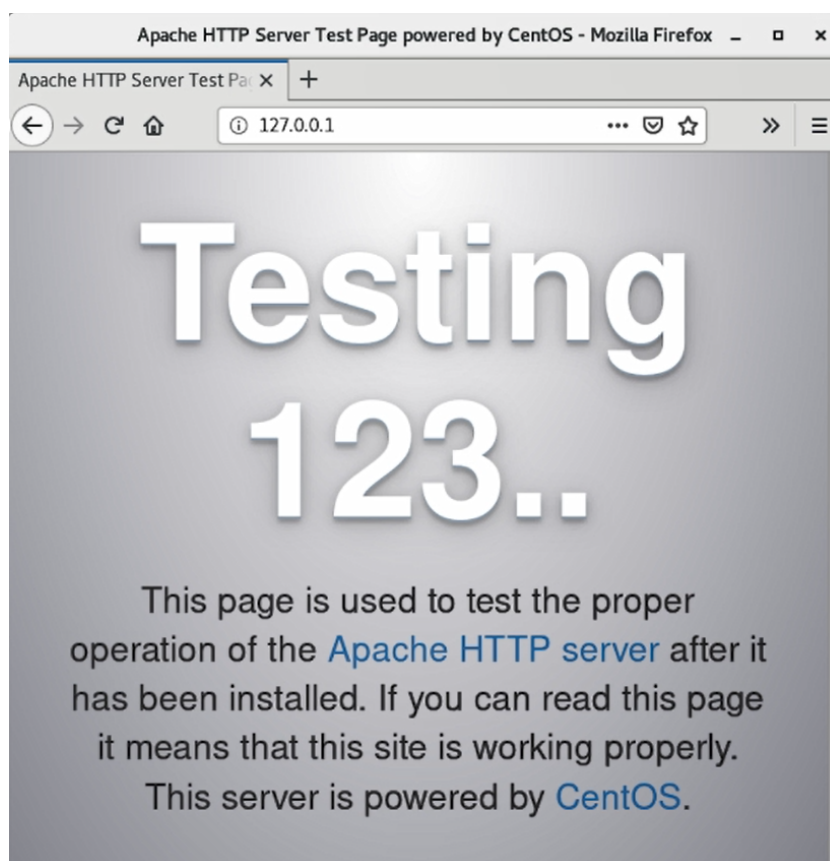


Figure 2.5: Проверка через браузер

```
[root@edikisakhayan conf]# 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: active (running) since Br 2022-09-20 18:38:28 MSK; 1s ago
     Docs: man:httpd(8)
    man:apachectl(8)
  Main PID: 6361 (httpd)
   Status: "Processing requests..."
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─6361 /usr/sbin/httpd -DFOREGROUND
             └─6371 /usr/sbin/httpd -DFOREGROUND
               └─6372 /usr/sbin/httpd -DFOREGROUND
                 └─6373 /usr/sbin/httpd -DFOREGROUND
                   └─6374 /usr/sbin/httpd -DFOREGROUND
                     └─6375 /usr/sbin/httpd -DFOREGROUND

сен 20 18:38:28 edikisakhayan.localdomain systemd[1]: Starting The Apache ...
сен 20 18:38:28 edikisakhayan.localdomain systemd[1]: Started The Apache H...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figure 2.6: Проверка статуса

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности. (рис. 2.7)


```

[root@edikisakhayan conf]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 6361 0.1 0.4 224084 5012 ? S
s 18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6371 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6372 0.0 0.3 226304 3828 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6373 0.0 0.3 226304 3832 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6374 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6375 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6427 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6442 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6443 0.0 0.3 226168 3096 ? S
18:38 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 root 6445 0.0 0.0 112832
972 pts/1 R+ 18:39 0:00 grep --color=auto httpd

```

Figure 2.7: веб-сервер Apache

Посмотрим текущее состояние переключателей SELinux для Apache. (рис. 2.8)

```

httpd_execmem off
httpd_graceful_shutdown on
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm I off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off

```

Figure 2.8: Просмотр переключателей SELinux для Apache

Посмотрим статистику по политике, также определил множество пользователей(8), ролей(14), типов(4793). (рис. 2.9)

```
[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 2.9: Статистика

Определим тип файлов и поддиректорий, находящихся в директории /var/www, также определим тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`, и определим круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 2.10)

```
[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 2.10: Определение типов файлов и круг пользователей

Создадим от имени суперпользователя html-файл /var/www/html/test.html. (рис. 2.11)

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

Figure 2.11: Создание файла

Проверим контекст созданного файла: `httpd_sys_content_t`. (рис. 2.12)

```
[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 2.12: Проверка

Обратимся к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедимся, что файл был успешно отображён. (рис. 2.13)

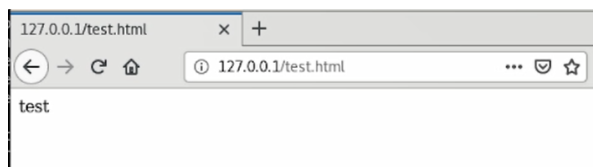


Figure 2.13: Получение доступа к файлу через браузер

Проверим контекст файла и изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверим, что контекст поменялся. (рис. 2.14)

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

Figure 2.14: Изменение контекста, проверка

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получим сообщение об ошибке. (рис. 2.15)

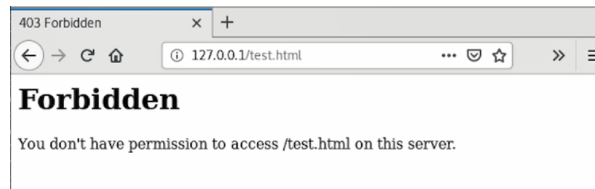


Figure 2.15: Получение доступа к файлу через браузер

Файл не был отображён потому что мы изменили контекст файла. Просмотрим log-файлы веб-сервера Apache. Также посмотрим системный лог-файл: `tail /var/log/messages`. (рис. 2.16)



Figure 2.16: Анализ ситуации

Попробуем 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` найдем строчку `Listen 80` и заменим её на `Listen 81`. (рис. 2.17)

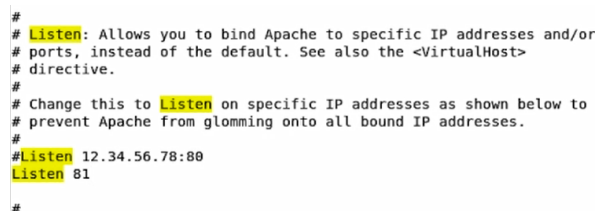


Figure 2.17: Изменеие порта 80 на 81

Просмотрим файл `/var/log/http/error_log`. (рис. 2.18)

```
[root@edikisakhayan html]# tail -n1 /var/log/messages
Sep 20 18:47:09 edikisakhayan dbus[733]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
```

Figure 2.18: Анализ и просмотр лог-файлов

Выполним команду: `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов. Убедимся, что порт 81 появился в списке. (рис. 2.19)

```
[root@edikisakhayan html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@edikisakhayan html]# 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@edikisakhayan html]# 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
```

Figure 2.19: Выполнение и проверка

Вернем 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`. Снова увидим содержимое файла — слово «test». (рис. 2.20 - 2.21)

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

Figure 2.20: Возвращение контекста

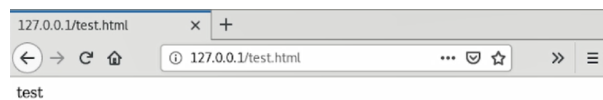


Figure 2.21: Получение доступа к файлу через браузер

Исправим обратно конфигурационный файл `apache`, вернув `Listen80`. (рис. 2.22)

```
#
# 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 80

#
# Dynamic Shared Object (DSO) Support
#
```

Figure 2.22: Исправленный файл `apache`

Удалим привязку `http_port_t` к 81 порту и удалим файл `/var/www/html/test.html`. (рис. 2.23)

```
[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 2.23: Удаление привязки к 81 порту и удаление файла

3 Выводы

В ходе работы, мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” <https://esystem.rudn.ru/>
::: {#refs} :::