

Отчёт лабораторной работы 6

Мандатное разграничение прав в Linux

Турсунов Баходурхон Азимджонович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	Подготовка	6
2.2	Изучение механики SetUID	6
3	Вывод	12

List of Figures

2.1	getenforce/sestatus	7
2.2	grep httpd	7
2.3	определение типа файлов	8
2.4	html-файл	8
2.5	открытие файла	8
2.6	веб-сервер	9
2.7	веб-сервер	9
2.8	log-файлы	10
2.9	semanage port	10
2.10	контекст	11

List of Tables

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Подготовка

1. Установил httpd
2. Задал имя сервера
3. Открыл порты для работы с протоколом http

2.2 Изучение механики SetUID

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере и убедился, что последний работает.

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost ~]# getenforce  
Enforcing  
[root@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  
[root@localhost ~]# 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 pres>  
   Active: inactive (dead)  
   Docs: man:httpd.service(8)  
lines 1-4/4 (END)
```

Figure 2.1: getenforce/sestatus

3. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности.

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost ~]# sestatus -b | grep httpd  
httpd_anon_write off  
httpd_builtin_scripting on  
httpd_can_check_spam off  
httpd_can_connect_ftp off  
httpd_can_connect_ldap off  
httpd_can_connect_mythtv off  
httpd_can_connect_zabbix off  
httpd_can_network_connect off  
httpd_can_network_connect_cobbler off  
httpd_can_network_connect_db off  
httpd_can_network_memcache off  
httpd_can_network_relay off  
httpd_can_sendmail off  
httpd_dbus_avaahi off  
httpd_dbus_sssd off  
httpd_dontaudit_search_dirs off  
httpd_enable_cgi on  
httpd_enable_ftp_server off  
httpd_enable_homedirs off  
httpd_execmem off  
httpd_graceful_shutdown off  
httpd_manage_ipa off  
httpd_mod_auth_ntlm_winbind off
```

Figure 2.2: grep httpd

4. Определил тип файлов и поддиректорий, находящихся в директории /var/www с помощью команды `ls -lZ /var/www`
5. Определил тип файлов, находящихся в директории /var/www/html с помощью команды `ls -lZ /var/www/html`

```

[root@localhost ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июн 22 14:26 cg
i-bin
drwxr-xr-x. 3 root root system_u:object_r:git_content_t:s0 38 сен 12 02:02 gi
t
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июн 22 14:26 ht
ml
[root@localhost ~]# ls -lZ /var/www/html/
итого 0

```

Figure 2.3: определение типа файлов

6. Создал от имени суперпользователя html-файл



The screenshot shows a text editor window titled "test.html" with the path "/var/www/html". The editor contains the following HTML code:

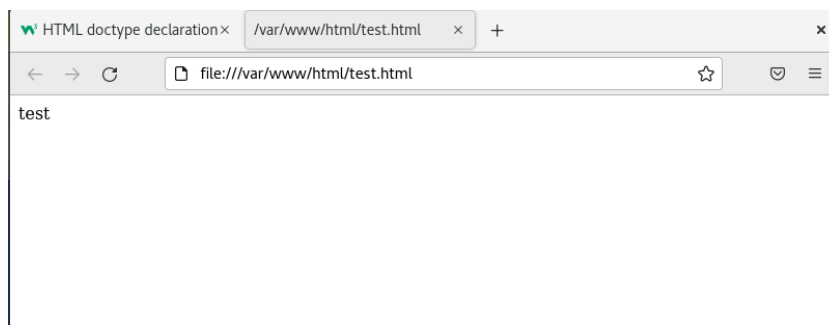
```

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

```

Figure 2.4: html-файл

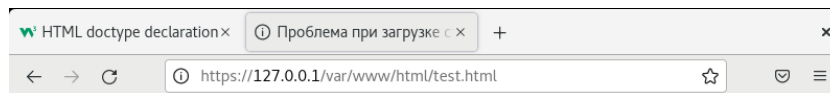
7. Открыв файл с помощью Chrome видим наш текст



The screenshot shows a Chrome browser window with the address bar displaying "file:///var/www/html/test.html". The page content is "test".

Figure 2.5: открытие файла

8. Обратившись к файлу через веб-сервер введя в браузере нужный адрес, получил ошибку.



Попытка соединения не удалась

Firefox не может установить соединение с сервером 127.0.0.1.

- Возможно, сайт временно недоступен или перегружен запросами. Подождите некоторое время и попробуйте снова.
- Если вы не можете загрузить ни одну страницу - проверьте настройки соединения с Интернетом.
- Если ваш компьютер или сеть защищены межсетевым экраном или прокси-сервером - убедитесь, что Firefox разрешён выход в Интернет.

Попробовать снова

Figure 2.6: веб-сервер

9. Изучил справку `man httpd_selinux`

10. Изменил контекст файла с `httpd_sys_content_t` на `samba_share_t`

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

Figure 2.7: веб-сервер

11. Снова попробовал доступ к файлу через веб-сервер и снова не получилось.

12. Просмотрел log-файлы веб-сервера Apache. Система предупреждает что она работает очень медленно.

```
[root@localhost ~]# tail /var/log/messages
Oct 13 19:02:41 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce: scheduled expiry is in the past (-38ms), your system
is too slow
Oct 13 19:02:41 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce short: scheduled expiry is in the past (-51ms), your
system is too slow
Oct 13 19:02:46 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce: scheduled expiry is in the past (-14ms), your system
is too slow
Oct 13 19:02:46 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce: scheduled expiry is in the past (-14ms), your system
is too slow
Oct 13 19:02:46 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce short: scheduled expiry is in the past (-27ms), your
system is too slow
Oct 13 19:02:53 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce: scheduled expiry is in the past (-14ms), your system
is too slow
Oct 13 19:02:53 localhost org.gnome.Shell.desktop[2144]: libinput error: client
bug: timer event4 debounce short: scheduled expiry is in the past (-27ms), your
system is too slow
```

Figure 2.8: log-файлы

13. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. И для этого в файле /etc/httpd/conf/httpd.conf нашел строчку Listen 80 и заменил ее на Listen 81.
14. Выполнил команду `semanage port -a -t http_port_t -p tcp 81`, и после этого проверил список портов командой `semanage port -l | grep http_port_t` и убедился, что порт 81 появился в списке.

```
[root@localhost ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@localhost ~]# sem
semanage      semodule_expand      semodule_package
semodule      semodule_link        semodule_unpackage
[root@localhost ~]# 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@localhost ~]# service apache start
Redirecting to /bin/systemctl start apache.service
Failed to start apache.service: Unit apache.service not found.
[root@localhost ~]# apache start
bash: apache: команда не найдена...
[root@localhost ~]# systemctl start httpd
bash: systemctl: команда не найдена...
Аналогичная команда: 'systemctl'
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl start apache
Failed to start apache.service: Unit apache.service not found.
[root@localhost ~]#
```

Figure 2.9: semanage port

15. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` командой `chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого

попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. и все равно получил ошибку

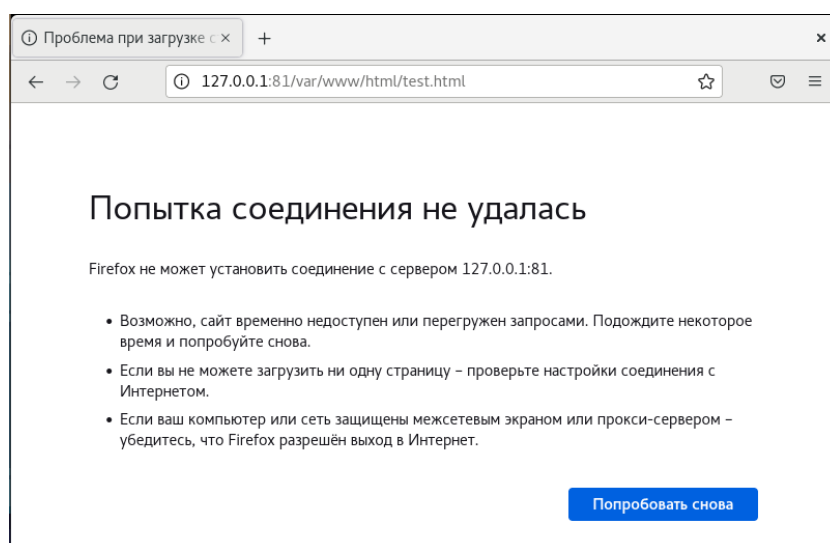


Figure 2.10: контекст

16. Удалил файл `/var/www/html/test.html` командой `rm /var/www/html/test.html`

3 Вывод

В процессе выполнения лабораторной работы были получены базовые навыки работы с технологией SELinux.