

# Отчёта по лабораторной работе №4

дисциплина: Информационная безопасность

Кашкин Иван Евгеньевич

## Содержание

Цель работы.....	
Задание .....	
Теоретическое введение .....	
Выполнение лабораторной работы .....	
Выводы.....	
Список литературы.....	

## Цель работы

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

## Выполнение лабораторной работы

### Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.

```
lekashkin@localhost:/home/lekashkin — /bin/systemctl status ...
• httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-10-12 15:50:15 MSK; 28min ago
  Docs: man:httpd.service(8)
  Main PID: 3376 (httpd)
  Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
  Tasks: 177 (limit: 10971)
  Memory: 9.7M
  CPU: 11.204s
  CGroup: /system.slice/httpd.service
          └─3376 /usr/sbin/httpd -DFOREGROUND
             └─3377 /usr/sbin/httpd -DFOREGROUND
                └─3378 /usr/sbin/httpd -DFOREGROUND
                   └─3379 /usr/sbin/httpd -DFOREGROUND
                      └─3380 /usr/sbin/httpd -DFOREGROUND

Oct 12 15:50:15 localhost.localdomain systemd[1]: Starting The Apache HTTP Server: httpd.
Oct 12 15:50:15 localhost.localdomain httpd[3376]: AH00558: httpd: Could not reconfigure.
Oct 12 15:50:15 localhost.localdomain httpd[3376]: Server configured, listening on *
Oct 12 15:50:15 localhost.localdomain systemd[1]: Started The Apache HTTP Server: httpd.
-
-
-
3. :3
```

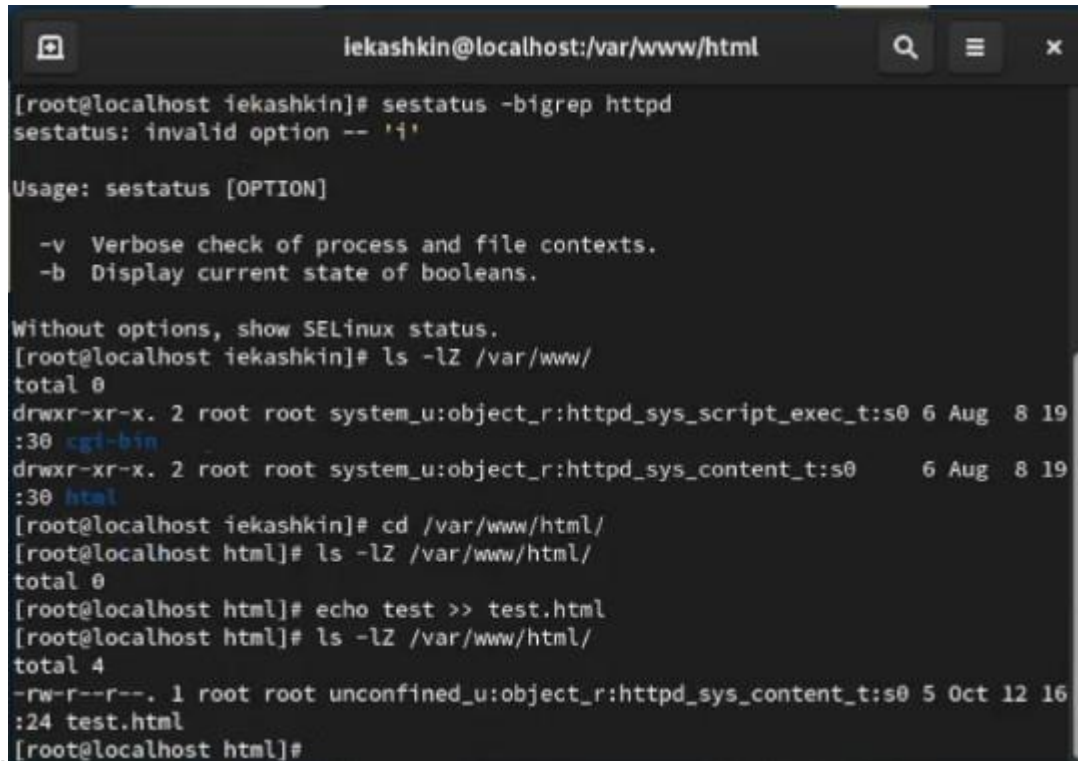
Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep`

httpd или ps -eZ | grep httpd

```
iekashkin@localhost:/home/iekashkin
[iekashkin@localhost ~]$ su
Password:
[root@localhost iekashkin]# ps aux -Z | grep http
system_u:system_r:httpd_t:s0 root 3376 0.0 0.4 20152 8108 ?
Ss 15:50 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3377 0.0 0.2 22032 5308 ?
S 15:50 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3378 0.2 0.3 2357772 5768 ?
Sl 15:50 0:03 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3379 0.2 0.3 2226636 5692 ?
Sl 15:50 0:03 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3380 0.2 0.3 2226636 5604 ?
Sl 15:50 0:03 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4497 0.0 0.1 221796
2432 pts/0 S+ 16:21 0:00 grep --color=auto http
[root@localhost iekashkin]#
```



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



```
iekashkin@localhost:/var/www/html
[root@localhost iekashkin]# 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.
[root@localhost iekashkin]# ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug  8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 Aug  8 19
:30 html
[root@localhost iekashkin]# cd /var/www/html/
[root@localhost html]# ls -lZ /var/www/html/
total 0
[root@localhost html]# echo test >> test.html
[root@localhost html]# ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Oct 12 16
:24 test.html
[root@localhost html]#
```

- 11.
12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
13. Измените 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 проверьте, что контекст поменялся.
14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server`. При изменении контекста файл стал считаться чужим для `http` и программа не может его прочитать.
15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `auditd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```
iekashkin@localhost:/var/www/html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Oct 12 16:24 test.html
[root@localhost html]# chcon -t samba_share_t test.html
[root@localhost html]# ls -lZ /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 5 Oct 12 16:24 test.html
[root@localhost html]# tail /var/log/messages
Oct 12 16:20:31 localhost systemd[1909]: Started GNOME Terminal Server.
Oct 12 16:20:31 localhost systemd[1909]: Started VTE child process 4431 launched by gnome-terminal-server process 4413.
Oct 12 16:20:35 localhost systemd[1]: Starting Fingerprint Authentication Daemon
...
Oct 12 16:20:35 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 16:20:36 localhost su[4458]: (to root) iekashkin on pts/0
Oct 12 16:21:05 localhost systemd[1]: fprintd.service: Deactivated successfully.
Oct 12 16:27:20 localhost systemd[1]: Starting Fingerprint Authentication Daemon
...
Oct 12 16:27:20 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Oct 12 16:27:23 localhost NetworkManager[892]: <info> [1728739643.4200] agent-manager: agent[069ba7b12faf1ef6,:1.68/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 12 16:27:50 localhost systemd[1]: fprintd.service: Deactivated successfully.
[root@localhost html]#
```

16.

17. Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81.

```
apbaranova@apbaranova:/var/www/html — mcedit /etc/httpd/conf/httpd.conf
httpd.conf [----] 9 L: [ 19+28 47/359] *(2025/12005b) 0010 0x00A
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# 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 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Пере~тить 7Поиск 8Удалить 9МенюМС
```

#fig

18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.
19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз.
21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1:81/test.html>. Вы должны увидеть содержимое файла — слово «test».



```
iekashkin@localhost:/var/www/html
Oct 12 16:27:23 localhost NetworkManager[892]: <info> [1728739643.4200] agent-m
anager: agent[069ba7b12faf1ef6,:1.68/org.gnome.Shell.NetworkAgent/1000]: agent r
egistered
Oct 12 16:27:50 localhost systemd[1]: fprintd.service: Deactivated successfully.
[root@localhost html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost html]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@localhost html]# semanage port -l | grep http
http_cache_port_t      tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t      udp      3130
http_port_t            tcp      81, 80, 81, 443, 488, 8008, 8009, 8443,
9000
pegasus_http_port_t    tcp      5988
pegasus_https_port_t   tcp      5989
[root@localhost html]# chcon -t http_sys_connect_t test.html
chcon: failed to change context of 'test.html' to 'unconfined_u:object_r:http_sy
s_connect_t:s0': Invalid argument
[root@localhost html]# chcon -t http_sys_connect_t test.html
chcon: failed to change context of 'test.html' to 'unconfined_u:object_r:http_sy
s_connect_t:s0': Invalid argument
[root@localhost html]# ls -Z
unconfined_u:object_r:samba_share_t:s0 test.html
[root@localhost html]#
```

#fig

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
23. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
24. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

## Выводы

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

## Список литературы{.unnumbered}

1. [SELinux в CentOS](#)
2. [Веб-сервер Apache](#)