

Основы информационной безопасности. Лабораторная работа №6

Мандатное разграничение прав в Linux

Демидова Е.А.

09.09.2023

Российский Университет дружбы народов

Информация

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/eademidova>



Вводная часть

Целью данной работы является приобретение практических навыков администрирования ОС Linux.

Задачи:

- Получить первое практическое знакомство с технологией SELinux.
- Проверить работу SELinux на практике совместно с веб-сервером Apache.

Инструмент: VirtualBox

Выполнение лабораторной работы

Подготовка лабораторного стенда

```
root@eademidova:~#
Installing      : rocky-logos-httpd-90.15-2.el9.noarch          9/14
Installing      : mod_http2-2.0.26-2.el9_4.x86_64             10/14
Installing      : httpd-2.4.57-8.el9.x86_64                   11/14
Running scriptlet: httpd-2.4.57-8.el9.x86_64                  11/14
Installing      : mod_ssl-1:2.4.57-8.el9.x86_64                12/14
Installing      : httpd-manual-2.4.57-8.el9.noarch              13/14
Installing      : mod_fcgid-2.3.9-28.el9.x86_64                14/14
Running scriptlet: httpd-2.4.57-8.el9.x86_64                  14/14
Running scriptlet: mod_fcgid-2.3.9-28.el9.x86_64              14/14
Verifying       : rocky-logos-httpd-90.15-2.el9.noarch         1/14
Verifying       : mod_ssl-1:2.4.57-8.el9.x86_64               2/14
Verifying       : mod_lua-2.4.57-8.el9.x86_64                 3/14
Verifying       : httpd-tools-2.4.57-8.el9.x86_64             4/14
Verifying       : httpd-2.4.57-8.el9.x86_64                   5/14
Verifying       : httpd-manual-2.4.57-8.el9.noarch             6/14
Verifying       : httpd-fsfilesystem-2.4.57-8.el9.noarch       7/14
Verifying       : apr-util-openssl-1.6.1-23.el9.x86_64         8/14
Verifying       : apr-util-bdb-1.6.1-23.el9.x86_64            9/14
Verifying       : apr-util-1.6.1-23.el9.x86_64                10/14
Verifying       : mod_http2-2.0.26-2.el9_4.x86_64             11/14
Verifying       : mod_fcgid-2.3.9-28.el9.x86_64               12/14
Verifying       : apr-1.7.0-12.el9_3.x86_64                   13/14
Verifying       : httpd-core-2.4.57-8.el9.x86_64              14/14

Installed:
apr-1.7.0-12.el9_3.x86_64      apr-util-1.6.1-23.el9.x86_64
apr-util-bdb-1.6.1-23.el9.x86_64  apr-util-openssl-1.6.1-23.el9.x86_64
httpd-2.4.57-8.el9.x86_64      httpd-core-2.4.57-8.el9.x86_64
httpd-fsfilesystem-2.4.57-8.el9.noarch  httpd-manual-2.4.57-8.el9.noarch
httpd-tools-2.4.57-8.el9.x86_64  mod_fcgid-2.3.9-28.el9.x86_64
mod_http2-2.0.26-2.el9_4.x86_64  mod_lua-2.4.57-8.el9.x86_64
mod_ssl-1:2.4.57-8.el9.x86_64  rocky-logos-httpd-90.15-2.el9.noarch

Complete!
[root@eademidova ~]# nano /etc/httpd/httpd.conf
[root@eademidova ~]# iptables -F
[root@eademidova ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
[root@eademidova ~]# iptables -P INPUT ACCEPT
[root@eademidova ~]# iptables -P OUTPUT ACCEPT
[root@eademidova ~]#
```

Рис. 1: Подготовка лабораторного стенда

```
root@eademidova:~  
httpd-tools-2.4.57-8.el9.x86_64      mod_fcgid-2.3.9-28.el9.x86_64  
mod_http2-2.0.26-2.el9_4.x86_64    mod_lua-2.4.57-8.el9.x86_64  
mod_ssl-1:2.4.57-8.el9.x86_64      rocky-logos-httpd-90.15-2.el9.noarch  
  
Complete!  
[root@eademidova ~]# nano /etc/httpd/httpd.conf  
[root@eademidova ~]# iptables -F  
[root@eademidova ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT  
Bad argument `iptables'  
Try `iptables -h' or `iptables --help' for more information.  
[root@eademidova ~]# iptables -P INPUT ACCEPT  
[root@eademidova ~]# iptables -P OUTPUT ACCEPT  
[root@eademidova ~]# getenforce  
Enforcing  
[root@eademidova ~]# 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
```

Рис. 2: Проверка статуса SELinux

Практическое знакомство с технологией SELinux

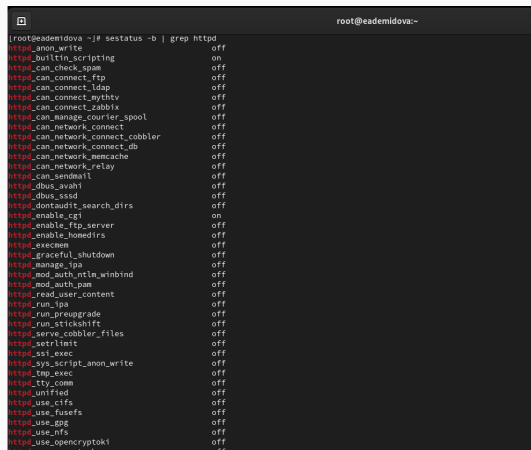
```
[root@eademidova ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
o httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[root@eademidova ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@eademidova ~]# systemctl start httpd
[root@eademidova ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sun 2024-07-07 18:01:01 MSK; 2s ago
     Docs: man:httpd.service(8)
  Main PID: 5409 (httpd)
    Status: "Started, listening on: port 443, port 80"
    Tasks: 178 (limit: 10966)
  Memory: 25.1M
    CPU: 58ms
  CGroup: /system.slice/httpd.service
          └─5409 /usr/sbin/httpd -DFOREGROUND
            └─5411 /usr/sbin/httpd -DFOREGROUND
              └─5412 /usr/sbin/httpd -DFOREGROUND
                └─5413 /usr/sbin/httpd -DFOREGROUND
                  └─5414 /usr/sbin/httpd -DFOREGROUND
                    └─5415 /usr/sbin/httpd -DFOREGROUND

Jul 07 18:01:01 eademidova.localdomain systemd[1]: Starting The Apache HTTP Server...
Jul 07 18:01:01 eademidova.localdomain systemd[1]: Started The Apache HTTP Server.
Jul 07 18:01:01 eademidova.localdomain httpd[5409]: Server configured, listening on: port 443, port 80
[root@eademidova ~]#
```

Рис. 3: Проверка статуса веб-сервера

```
[root@eademidova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 5409 0.0 0.9 23544 16588 ? Ss 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 5411 0.0 0.4 24248 8204 ? S 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 5412 0.0 0.4 25596 7308 ? S 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 5413 0.0 0.6 984852 12088 ? Sl 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 5414 0.0 0.7 1115988 14536 ? Sl 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 5415 0.0 0.6 984852 12076 ? Sl 18:01 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 5610 0.0 0.1 221664 2304 pts/0 S+ 18:03 0:00 grep --color=auto httpd
[root@eademidova ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 5409 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 5411 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 5412 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 5413 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 5414 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 5415 ? 00:00:00 httpd
[root@eademidova ~]#
```

Рис. 4: Просмотр контекста безопасности веб-сервера

A terminal window with a dark background. The prompt is 'root@eademidova:~'. The command executed is 'sestatus -b | grep httpd'. The output is a list of SELinux booleans for the httpd process, each followed by its status (on or off).

```
root@eademidova:~# 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_manage_courier_spool 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
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 off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
```

Рис. 5: Состояние переключателей SELinux для Apache

```
zarara_domain
[root@eademidova ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Permissions:             457
Sensitivities:           1
Categories:              1024
Types:                   5145
Attributes:              259
Users:                   8
Roles:                   15
Booleans:                356
Cond. Expr.:            388
Allow:                   65500
Neverallow:              0
Auditallow:              176
Dontaudit:               8682
Type_trans:              271770
Type_change:             94
Type_member:             37
Range_trans:             5931
Role_allow:              40
Role_trans:              417
Constraints:             70
Validatetrans:           0
MLS Constrain:           72
MLS Val. Tran:           0
Permissives:             4
Polcap:                  6
Defaults:                7
Typebounds:              0
Allowxperm:              0
Neverallowxperm:         0
Auditallowxperm:         0
Dontauditxperm:          0
Ibendportcon:            0
Ibpkeycon:               0
Initial SIDs:            27
Fs_use:                  35
Genfscon:                109
Portcon:                 665
Netifcon:                0
Nodecon:                 0
[root@eademidova ~]# seinfo -u
```

Рис. 6: Статистика по политике



```
Net11rcon: 0 Nodecon: 0
[root@eademidova ~]# seinfo -u

Users: 8
  guest_u
  root
  staff_u
  sysadm_u
  system_u
  unconfined_u
  user_u
  xguest_u
[root@eademidova ~]# seinfo -r

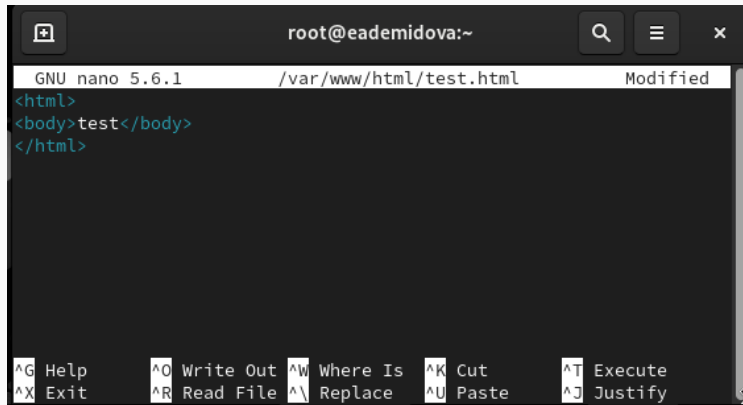
Roles: 15
  auditadm_r
  container_user_r
  dbadm_r
  guest_r
  logadm_r
  nx_server_r
  object_r
  secadm_r
  staff_r
  sysadm_r
  system_r
  unconfined_r
  user_r
  webadm_r
  xguest_r
[root@eademidova ~]# seinfo -t

Types: 5145
  NetworkManager_dispatcher_chronyc_script_t
  NetworkManager_dispatcher_chronyc_t
  NetworkManager_dispatcher_cloud_script_t
  NetworkManager_dispatcher_cloud_t
  NetworkManager_dispatcher_console_script_t
  NetworkManager_dispatcher_console_t
  NetworkManager_dispatcher_console_var_run_t
  NetworkManager_dispatcher_custom_t
  NetworkManager_dispatcher_ddclient_script_t
  NetworkManager_dispatcher_ddclient_t
```

Рис. 7: Множества пользователей, ролей, типов

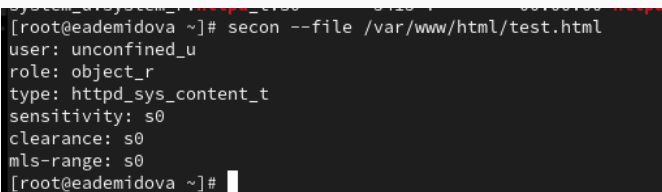
```
[root@eademidova ~]# ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Apr 22 04:04 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Apr 22 04:04 html
[root@eademidova ~]# ls -lZ /var/www/html/
total 0
[root@eademidova ~]#
```

Рис. 8: Просмотр типов директорий в /var/www



```
root@eademidova:~  
GNU nano 5.6.1 /var/www/html/test.html Modified  
<html>  
<body>test</body>  
</html>  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Рис. 9: Содержимое html-файла /var/www/html/test.html

A terminal window with a dark background. The prompt is [root@eademidova ~]#. The command 'secon --file /var/www/html/test.html' has been entered. The output shows SELinux policy details for the file: user: unconfined_u, role: object_r, type: httpd_sys_content_t, sensitivity: s0, clearance: s0, and mls-range: s0. The prompt is now [root@eademidova ~]# with a cursor.

```
[root@eademidova ~]# secon --file /var/www/html/test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[root@eademidova ~]#
```

Рис. 10: Установка пароля для пользователя с правами администратора

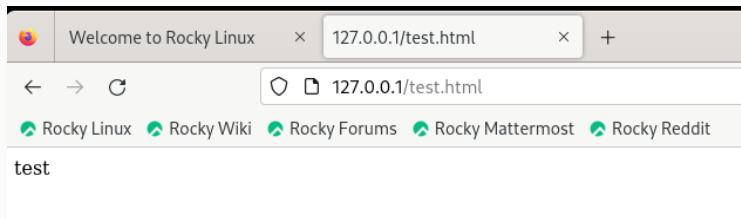


Рис. 11: Открытие html-страницы через браузер

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

Рис. 12: Изменение контекста файла /var/www/html/test.html

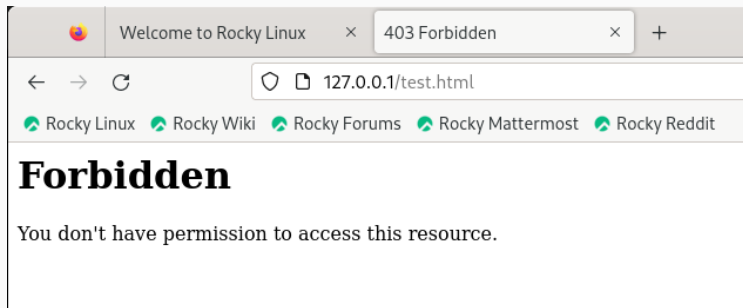
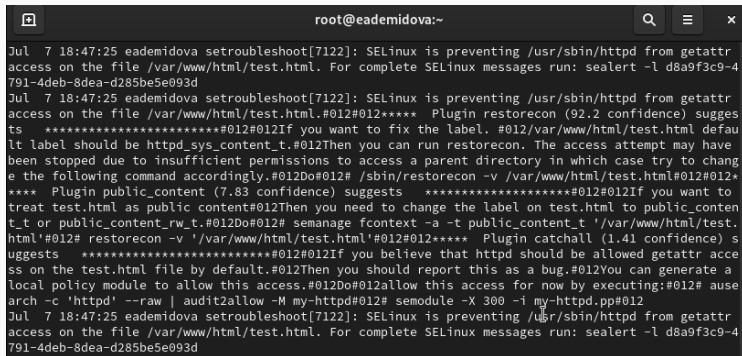
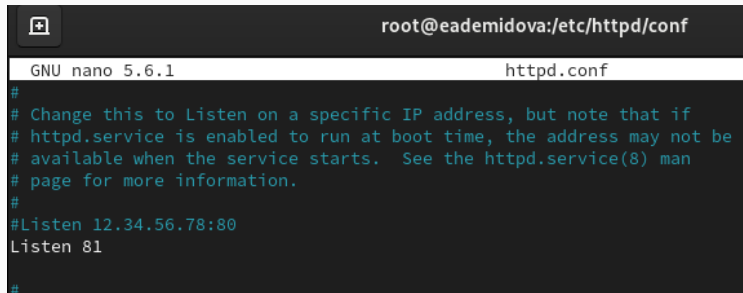


Рис. 13: Отказ в доступе к html-странице через браузер

A screenshot of a terminal window titled 'root@eademidova:~'. The terminal displays SELinux audit logs. The first log entry shows a denial for httpd to access a file in /var/www/html. The second log entry is a detailed message from the 'setroubleshoot' tool, suggesting the use of 'restorecon' to fix the label on the file. The third log entry shows another denial for httpd. The terminal window has a dark background and standard window controls at the top.

```
root@eademidova:~
Jul  7 18:47:25 eademidova setroubleshoot[7122]: SELinux is preventing /usr/sbin/httpd from getattr
access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l d8a9f3c9-4
791-4deb-8dea-d285be5e093d
Jul  7 18:47:25 eademidova setroubleshoot[7122]: SELinux is preventing /usr/sbin/httpd from getattr
access on the file /var/www/html/test.html.#012#012**** Plugin restorecon (92.2 confidence) sugges
ts *****#012#012If you want to fix the label. #012/var/www/html/test.html defau
lt label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have
been stopped due to insufficient permissions to access a parent directory in which case try to chang
e the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*
**** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to
treat test.html as public content#012Then you need to change the label on test.html to public_conten
t_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.
html'#012# restorecon -v '/var/www/html/test.html'#012#012**** Plugin catchall (1.41 confidence) s
uggests *****#012#012If you believe that httpd should be allowed getattr acce
ss on the test.html file by default.#012Then you should report this as a bug.#012You can generate a
local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ause
arch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Jul  7 18:47:25 eademidova setroubleshoot[7122]: SELinux is preventing /usr/sbin/httpd from getattr
access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l d8a9f3c9-4
791-4deb-8dea-d285be5e093d
```

Рис. 14: Просмотр лог-файлов



```
root@eademidova:/etc/httpd/conf
GNU nano 5.6.1 httpd.conf
#
# 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
#
```

Рис. 15: Замена прослушиваемого порта

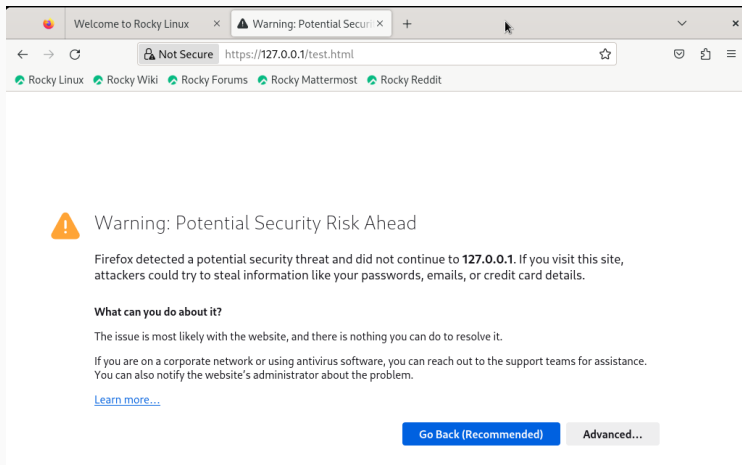
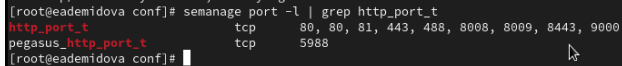


Рис. 16: Открытие html-страницы через браузер при прослушивании 81 порта

```
[root@eademidova conf]# tail -l /var/log/messages
Jul  7 19:11:09 eademidova systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@3.service: Deactivated successfully.
Jul  7 19:11:09 eademidova systemd[1]: setroubleshoold.service: Deactivated successfully.
Jul  7 19:11:15 eademidova systemd[1]: One-time temporary TLS key generation for httpd.service was skipped because no trigger condition checks were met.
Jul  7 19:12:28 eademidova systemd[1]: Stopping The Apache HTTP Server...
Jul  7 19:12:29 eademidova systemd[1]: httpd.service: Deactivated successfully.
Jul  7 19:12:29 eademidova systemd[1]: Stopped The Apache HTTP Server.
Jul  7 19:13:01 eademidova systemd[1]: One-time temporary TLS key generation for httpd.service was skipped because no trigger condition checks were met.
Jul  7 19:13:01 eademidova systemd[1]: Starting The Apache HTTP Server...
Jul  7 19:13:01 eademidova systemd[1]: Started The Apache HTTP Server.
Jul  7 19:13:01 eademidova httpd[8507]: Server configured, listening on: port 443, port 81
```

Рис. 17: Просмотр лог-файлов

A terminal window showing the command 'semanage port -l | grep http_port_t' and its output. The output lists two SELinux ports: 'http_port_t' for TCP on ports 80, 81, 443, 488, 8008, 8009, 8443, and 9000; and 'pegasus_http_port_t' for TCP on port 5988. The prompt is '[root@eademidova conf]#'.

```
[root@eademidova conf]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@eademidova conf]#
```

Рис. 18: Просмотр портов с помощью semanage

Заключение

В результате выполнения работы были приобретены практические навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работа SELinux на практике совместно с веб-сервером Apache.

SELinux – описание и особенности работы с системой. Часть 1 [Электронный ресурс]. Habr, 2014. URL: <https://habr.com/ru/companies/kingservers/articles/209644/>.