

Лабораторная работа №6

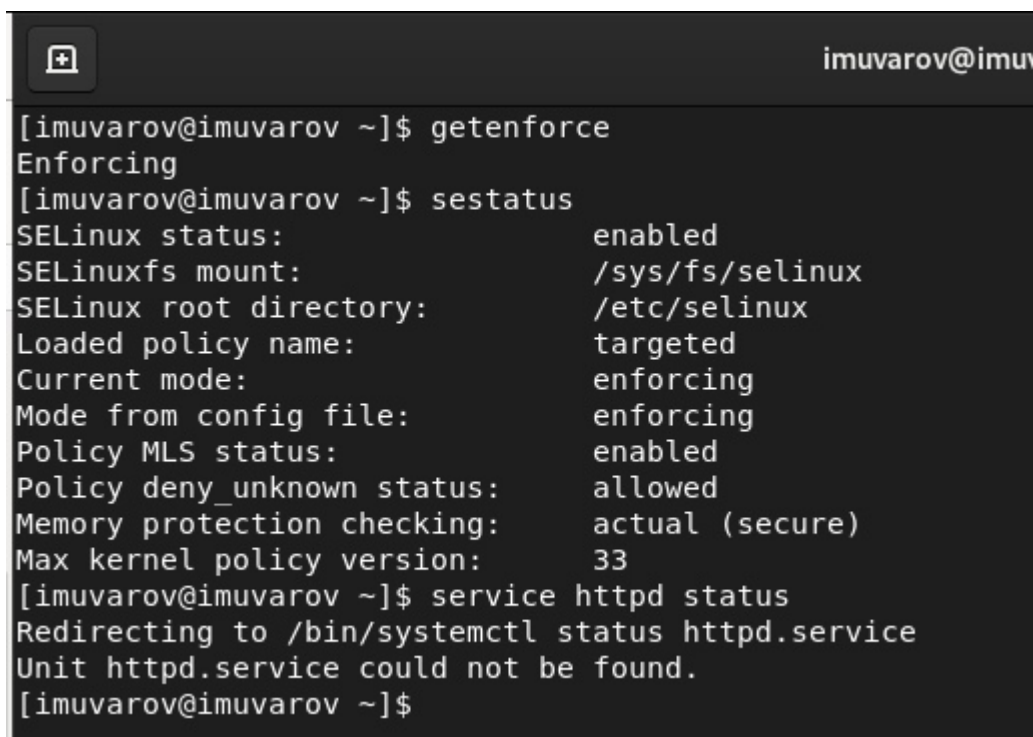
Уваров Илья НПИбд-02-19

Цель работы

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

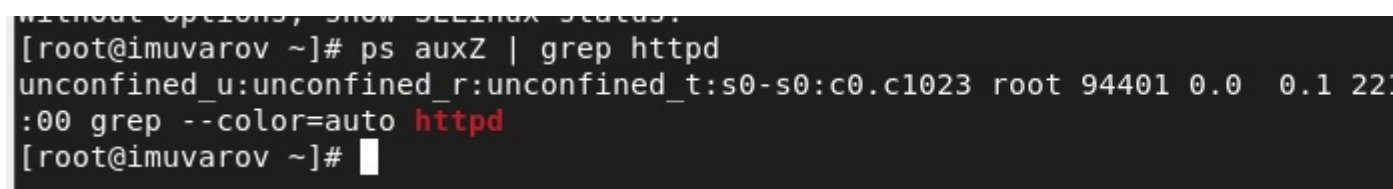
Выполнение лабораторной работы

1. Вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает (рис. 1).



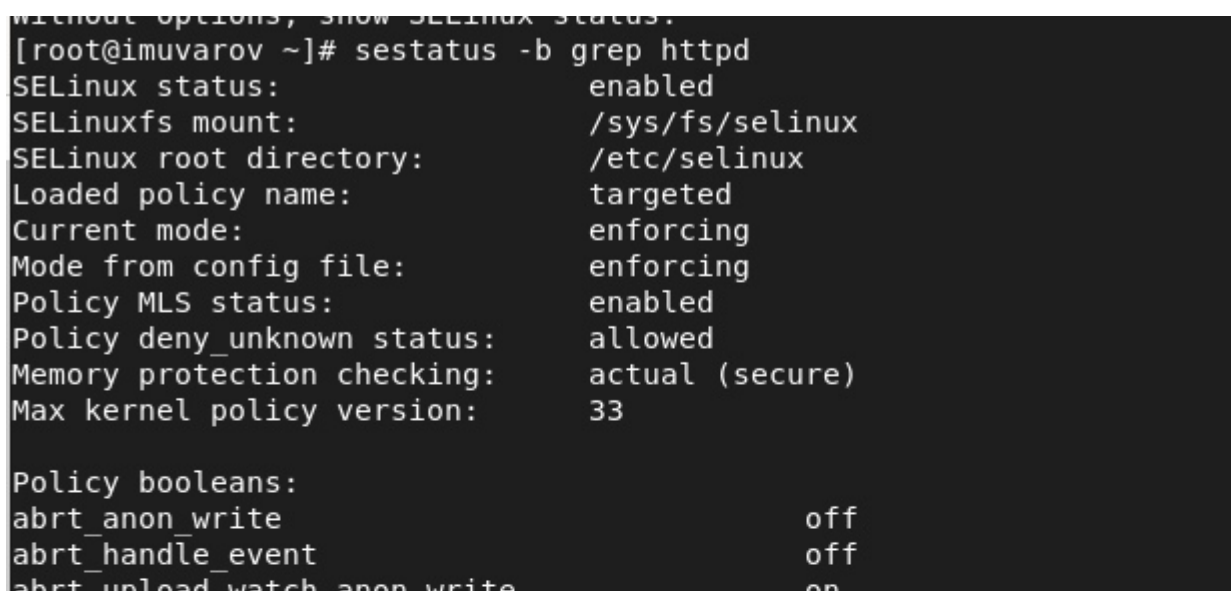
```
[imuvarov@imuvarov ~]$ getenforce
Enforcing
[imuvarov@imuvarov ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[imuvarov@imuvarov ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
[imuvarov@imuvarov ~]$
```

2. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности (рис. 2).



```
without options, show SELinux status.
[root@imuvarov ~]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 94401 0.0  0.1 22:
:00 grep --color=auto httpd
[root@imuvarov ~]#
```

3. Посмотрел текущее состояние переключателей SELinux для Apache (рис. 3).



```
without options, show SELinux status.
[root@imuvarov ~]# sestatus -b grep httpd
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

Policy booleans:
abrt_anon_write                 off
abrt_handle_event               off
abrt_upload_watch_anon_write    on
```

abrt_upload_watch_anon_write	on
antivirus_can_scan_system	off
antivirus_use_jit	off
auditadm_exec_content	on
authlogin_nsswitch_use_ldap	off
authlogin_radius	off
authlogin_yubikey	off
awstats_purge_apache_log_files	off
boinc_execmem	on
cdrecord_read_content	off
cluster_can_network_connect	off
cluster_manage_all_files	off
cluster_use_execmem	off
cobbler_anon_write	off
cobbler_can_network_connect	off
cobbler_use_cifs	off
cobbler_use_nfs	off
collectd_tcp_network_connect	off
colord_use_nfs	off
condor_tcp_network_connect	off
conman_can_network	off
conman_use_nfs	off
container_connect_any	off
container_manage_cgroup	off
container_use_cephfs	off
container_use_devices	off
cron_can_relabel	off
cron_system_cronjob_use_shares	off
cron_userdomain_transition	on
cups_execmem	off
cvs_read_shadow	off
daemons_dontaudit_scheduling	on
daemons_dump_core	off
daemons_enable_cluster_mode	off
daemons_use_tcp_wrapper	off
daemons_use_tty	off
dbadm_exec_content	on
dbadm_manage_user_files	off
dbadm_read_user_files	off
deny_bluetooth	off
deny_execmem	off
deny_ptrace	off
dhcpc_exec_iptables	off
dhcpd_use_ldap	off
dnsmasq_use_ipset	off
domain_can_mmap_files	off
domain_can_write_kmsg	off
domain_fd_use	on
domain_kernel_load_modules	off
entropyd_use_audio	on
exim_can_connect_db	off
exim_manage_user_files	off
exim_read_user_files	off
fcron_crond	off
fenced_can_network_connect	off
fenced_can_ssh	off
fips_mode	on
ftpd_anon_write	off

-
4. Посмотрел статистику по политике с помощью команды `seinfo`, также определил множество пользователей, ролей, типов (рис. 4).

```
[root@imuvarov ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

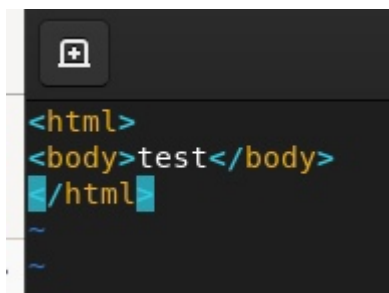
Classes:          133      Permissions:          454
Sensitivities:    1        Categories:          1024
Types:            5002     Attributes:           254
Users:            8        Roles:                14
Booleans:         347     Cond. Expr.:         381
Allow:            63996    Neverallow:           0
Auditallow:       168     Dontaudit:           8417
Type_trans:       258486   Type_change:          87
Type_member:       35     Range_trans:         5960
Role_allow:        38     Role_trans:          420
Constraints:       72     Validatetrans:        0
MLS Constrain:    72     MLS Val. Tran:        0
Permissives:       0      Polcap:               5
Defaults:         7      Typebounds:           0
Allowxperm:        0      Neverallowxperm:      0
Auditallowxperm:   0      Dontauditxperm:       0
Ibendportcon:      0      Ibpkeycon:            0
Initial SIDs:      27     Fs_use:               33
Genfscon:          106    Portcon:              651
Netifcon:          0      Nodecon:              0

[root@imuvarov ~]#
```

-
5. Определил тип файлов и поддиректорий, находящихся в директории `/var/www`. Определил тип файлов, находящихся в директории `/var/www/html`. Определил круг пользователей, которым разрешено создание файлов в директории (рис. 5).

```
[root@imuvarov ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16
[root@imuvarov ~]# ls -lZ /var/www/html
total 0
[root@imuvarov ~]#
```

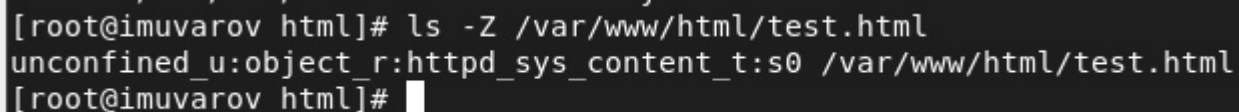
-
6. Создал от имени суперпользователя html-файл (рис. 6).

A screenshot of a code editor with a dark background. At the top left, there is a small icon of a square with a plus sign inside. Below it, the following HTML code is written in a light blue font:

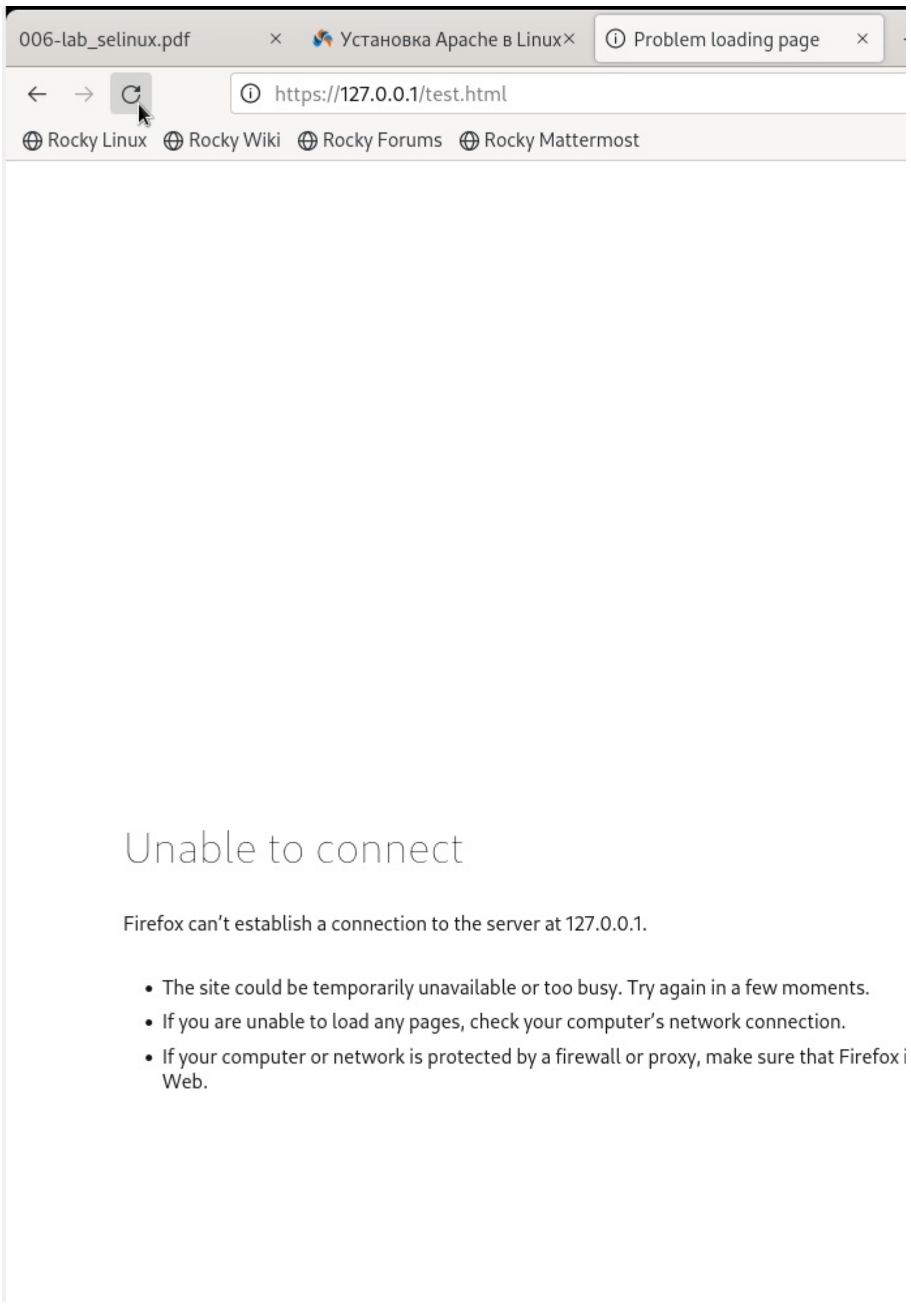
```
<html>
<body>test</body>
</html>
```

 There are two blue cursor lines visible on the left side of the editor, one on the line containing `</body>` and another on the line containing `</html>`.

7. Проверил контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `httpd_sys_content` (рис. 7).

A screenshot of a terminal window with a dark background. The prompt is `[root@imuvarov html]#`. The command `ls -Z /var/www/html/test.html` has been entered. The output is `unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html`. The prompt `[root@imuvarov html]#` is visible again at the bottom, followed by a white cursor block.

8. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Файл не отображён(рис. 8).



Unable to connect

Firefox can't establish a connection to the server at 127.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Internet.

9. Изменил контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t. После этого проверил, что контекст поменялся (рис. 9).

```
[root@imuvarov html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@imuvarov html]# vim /var/www/html/test.html
[root@imuvarov html]# chcon -t samba_share_t /var/www/html/test.html
[root@imuvarov html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@imuvarov html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Nov 15 17:05 /var/www/html/test.html
[root@imuvarov html]# tail /var/log/messages
Nov 15 17:19:04 imuvarov firefox.desktop[2196]: [Parent 2196, IPC I/O Parent
  destroyed with unconsumed descriptors: file /builddir/build/BUILD/firefox-9
me/common/file_descriptor_set_posix.cc:19
Nov 15 17:19:11 imuvarov systemd[1367]: Starting Portal service...
Nov 15 17:19:11 imuvarov systemd[1367]: Starting flatpak document portal ser
Nov 15 17:19:11 imuvarov systemd[1367]: Started flatpak document portal serv
Nov 15 17:19:11 imuvarov systemd[1367]: Starting Portal service (GTK/GNOME i
Nov 15 17:19:11 imuvarov systemd[1367]: Started Portal service (GTK/GNOME im
Nov 15 17:19:11 imuvarov systemd[1367]: Started Portal service.
Nov 15 17:19:13 imuvarov rtkit-daemon[743]: Successfully made thread 95274 o
firefox/firefox) owned by '1000' RT at priority 10.
Nov 15 17:19:20 imuvarov firefox.desktop[95140]: Missing chrome or resource
UpdateListener.js
Nov 15 17:19:20 imuvarov firefox.desktop[95140]: Missing chrome or resource
UpdateListener.sys.mjs
[root@imuvarov html]#
```

10. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 10).

<https://127.0.0.1/test.html>[Rocky Linux](#) [Rocky Wiki](#) [Rocky Forums](#) [Rocky Mattermost](#)

Unable to connect

An error occurred during a connection to 127.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox Web.

11. Проанализировал ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрел log-файлы веб-сервера Apache. Также посмотрите системный лог-файл. 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 (рис. 11).

```
[root@imuvarov html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Nov 15 17:05 /var/www/html/test.html
[root@imuvarov html]# tail /var/log/messages
Nov 15 17:19:04 imuvarov firefox.desktop[2196]: [Parent 2196, IPC I/O Parent]
destroyed with unconsumed descriptors: file /buildddir/build/BUILD/firefox-91
me/common/file_descriptor_set_posix.cc:19
Nov 15 17:19:11 imuvarov systemd[1367]: Starting Portal service...
Nov 15 17:19:11 imuvarov systemd[1367]: Starting flatpak document portal serv
Nov 15 17:19:11 imuvarov systemd[1367]: Started flatpak document portal servi
Nov 15 17:19:11 imuvarov systemd[1367]: Starting Portal service (GTK/GNOME in
Nov 15 17:19:11 imuvarov systemd[1367]: Started Portal service (GTK/GNOME imp
Nov 15 17:19:11 imuvarov systemd[1367]: Started Portal service.
Nov 15 17:19:13 imuvarov rtkit-daemon[743]: Successfully made thread 95274 of
firefox/firefox) owned by '1000' RT at priority 10.
Nov 15 17:19:20 imuvarov firefox.desktop[95140]: Missing chrome or resource U
UpdateListener.jsm
Nov 15 17:19:20 imuvarov firefox.desktop[95140]: Missing chrome or resource U
UpdateListener.sys.mjs
[root@imuvarov html]#
```

12. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Файл `/etc/httpd/httpd.conf` пуст. Видимо при установке Apache произошли ошибки.

Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.