

Лабораторная работа №6

Мандатное разграничение прав в Linux

Кекишева А.Д.

10 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Кекишева Анастасия Дмитриевна
- Бизнес-информатика
- Кафедра теории вероятности и кибербезопасности
- Российский университет дружбы народов
- 1032201194@pfur.ru
- <https://github.com/adkekisheva>

Цель работы

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

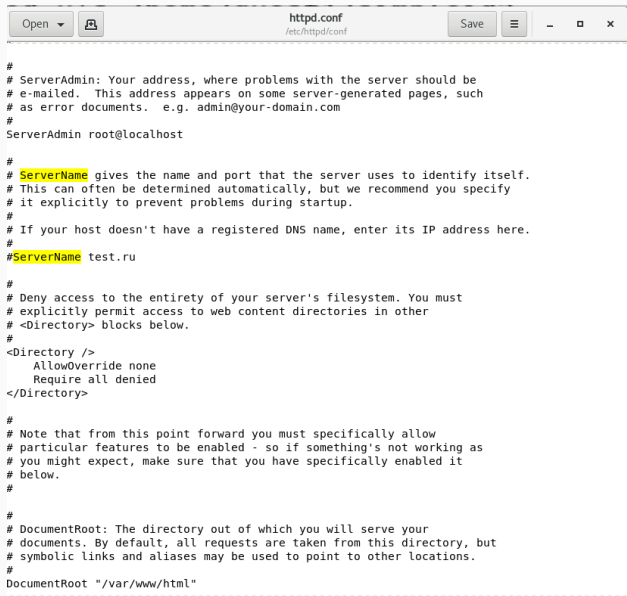
Задание

Выполнить последовательность действий описанных в лабораторной работе №6.

Выполнение лабораторной работы

Шаг 1





```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
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

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
```

Шаг 2

```
[root@adkekisheva conf]# iptables -F
[root@adkekisheva conf]# iptables -P INPUT ACCEPT
[root@adkekisheva conf]# getenforce
Enforcing
[root@adkekisheva 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
```

Рис. 2: Отключение пакетного фильтра и вход в систему

Шаг 3



```
[root@adkekisheva 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 preset: disabled)
   Active: active (running) since Mon 2023-10-02 21:15:10 MSK; 6 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 28449 (httpd)
    Status: "Total requests: 3; Current requests/sec: 0; Current traffic:  0 B/sec"
     Tasks: 7
    CGroup: /system.slice/httpd.service
            └─28449 /usr/sbin/httpd -DFOREGROUND
              └─28454 /usr/sbin/httpd -DFOREGROUND
                └─28455 /usr/sbin/httpd -DFOREGROUND
                  └─28456 /usr/sbin/httpd -DFOREGROUND
                    └─28457 /usr/sbin/httpd -DFOREGROUND
                      └─28458 /usr/sbin/httpd -DFOREGROUND
                        └─28542 /usr/sbin/httpd -DFOREGROUND

Oct 02 21:15:10 adkekisheva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 02 21:15:10 adkekisheva.localdomain httpd[28449]: AH00558: httpd: Could not reliably dete...ge
Oct 02 21:15:10 adkekisheva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Рис. 3: Проверка статуса веб-сервера

Шаг 4

```
[root@adkekisheva ~]# ps -auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 15236 0.0 0.0 112812 980 pts/6 R+ 15:1
2 0:00 grep --color=auto httpd
system_u:system_r:httpd_t:s0 root 28449 0.0 0.0 230448 432 ? Ss Oct08 0:06 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28454 0.0 0.0 232532 64 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28455 0.0 0.0 232532 40 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28456 0.0 0.0 232532 40 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28457 0.0 0.0 232668 68 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28458 0.0 0.0 232668 80 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 28542 0.0 0.0 232532 40 ? S Oct08 0:00 /
usr/sbin/httpd -DFOREGROUND
```

Рис. 4: Список процессов

Шаг 5



```
[root@adkekisheva ~]# 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_avahi 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 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
```

Шаг 6



```
[root@adkekiševa ~]# 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
```

Рис. 6: Статистика - команда seinfo

Шаг 7

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

Рис. 7: Определение типов файлов

Шаг 8

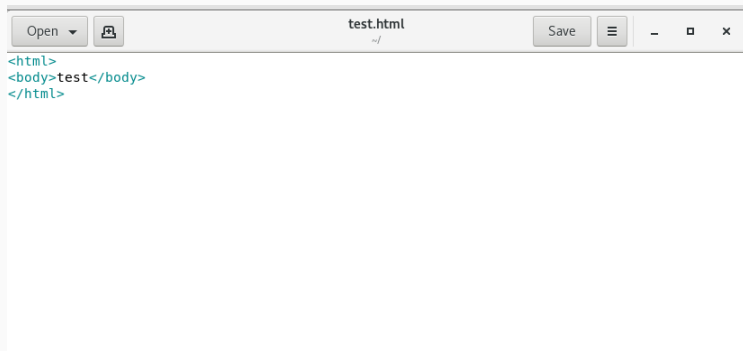


Рис. 8: Файл test.html

Шаг 9

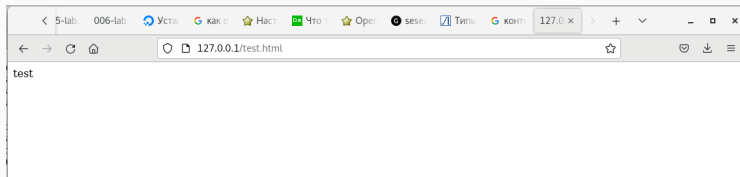


Рис. 9: Отображение содержимого файла в браузере

Шаг 10

```

root@adkekisheva:~
File Edit View Search Terminal Help
the httpd_suexec_t domain.

Paths:
    /usr/lib/apache(2)?/suexec(2)?, /usr/lib/cgi-bin/(nph-)?cgiwrap(d)?, /usr/sbin/suexec

httpd_suexec_tmp_t

- Set files with the httpd_suexec_tmp_t type, if you want to store httpd suexec temporary
  files in the /tmp directories.

httpd_sys_content_t

- Set files with the httpd_sys_content_t type, if you want to treat the files as httpd sys
  content.

Paths:
    /srv/([~]*)?www(/.*)?, /var/www(/.*)?, /etc/htdig(/.*)?, /srv/gallery2(/.*)?,
    /var/lib/trac(/.*)?, /var/lib/htdig(/.*)?, /var/www/icons(/.*)?,
    /usr/share/glpi(/.*)?, /usr/share/htdig(/.*)?, /usr/share/drupal.*, /usr/share/z-
    push(/.*)?, /var/www/svn/conf(/.*)?, /usr/share/icecast(/.*)?,
    /var/lib/cacti/rra(/.*)?, /usr/share/ntop/html(/.*)?, /usr/share/nginx/html(/.*)?,
    /usr/share/doc/ghc/html(/.*)?, /usr/share/openca/htdocs(/.*)?, /usr/share/selinux-pol-
    icy[~]*/html(/.*)?

httpd_sys_htaccess_t

- Set files with the httpd_sys_htaccess_t type, if you want to treat the file as a httpd
  sys access file.

httpd_sys_ra_content_t

- Set files with the httpd_sys_ra_content_t type, if you want to treat the files as httpd
  sys read/append content.

httpd_sys_rw_content_t

- Set files with the httpd_sys_rw_content_t type, if you want to treat the files as httpd
  sys read/write content.

Paths:
    /etc/glpi(/.*)?, /etc/horde(/.*)?, /etc/drupal.*, /etc/z-push(/.*)?,
    /var/lib/svn(/.*)?, /var/www/svn(/.*)?, /etc/owncloud(/.*)?,
    /var/www/html(/.*)?/uploads(/.*)?, /var/www/html(/.*)?/wp-content(/.*)?,

```

Шаг 11



```
[root@adkekisheva ~]# chcon -t samba_share_t /var/www/html/test.html
[root@adkekisheva ~]# s -Z /var/www/html/test.html
bash: s: command not found...
[root@adkekisheva ~]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 11: Команда chcon

Шаг 12



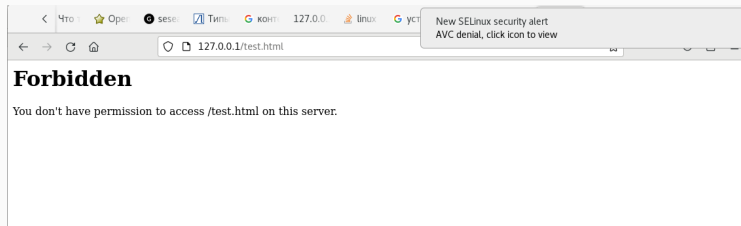


Рис. 12: Отказ в доступе - сообщение об ошибке от браузера

Шаг 13



```
[root@adkekisheva conf]# tail /var/log/messages
Oct 10 10:11:10 adkekisheva systemd: Starting Fingerprint Authentication Daemon...
Oct 10 10:11:10 adkekisheva dbus[718]: [system] Successfully activated service 'net.reactivated.Fingerprint'
Oct 10 10:11:10 adkekisheva systemd: Started Fingerprint Authentication Daemon.
Oct 10 10:11:14 adkekisheva NetworkManager[886]: <info> [1696921874.4907] agent-manager: req[0x55f01b3f4280, :1.61/org.gnome.Shell.NetworkAgent/1000]: agent registered
Oct 10 10:11:14 adkekisheva dbus[718]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 10 10:11:14 adkekisheva systemd: Starting Hostname Service...
Oct 10 10:11:14 adkekisheva dbus[718]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct 10 10:11:14 adkekisheva systemd: Started Hostname Service.
Oct 10 10:14:02 adkekisheva journal: Failed to open file "/home/adkekisheva/.cache/thumbnails/normal/24b9406ce5a0e0d87929bb8b9b055e17.png": No such file or directory
Oct 10 10:14:40 adkekisheva org.gnome.Shell.desktop: Window manager warning: Buggy client sent a _NET_ACTIVE_WINDOW message with a timestamp of 0 for 0x4400f8 (httpd.conf)
```

Рис. 13: Просмотр системных лог-файлов

Шаг 14



```

root@adkekisheva:/etc/httpd/conf
File Edit View Search Terminal Help
GNU nano 2.3.1 File: httpd.conf Modified

#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf

#
# If you wish httpd to run as a different user or group, you must run

```

Шаг 15



```

[root@adkekisheva conf]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@adkekisheva conf]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@adkekisheva 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 preset: disabled)
   Active: active (running) since Tue 2023-10-10 10:24:11 MSK; 1s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 29886 (httpd)
    Status: "Processing requests..."
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─29886 /usr/sbin/httpd -DFOREGROUND
              └─29890 /usr/sbin/httpd -DFOREGROUND
                └─29891 /usr/sbin/httpd -DFOREGROUND
                  └─29892 /usr/sbin/httpd -DFOREGROUND
                    └─29893 /usr/sbin/httpd -DFOREGROUND
                      └─29894 /usr/sbin/httpd -DFOREGROUND

Oct 10 10:24:11 adkekisheva.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 10 10:24:11 adkekisheva.localdomain httpd[29886]: AH00558: httpd: Could not reliably dete...ge
Oct 10 10:24:11 adkekisheva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@adkekisheva conf]# █

```

Рис. 15: Перезапуск Apache

Шаг 16



```

root@adkekisheva:~
File Edit View Search Terminal Help
ocaluser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1695723601.768:6041): pid=3736 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1695723601.768:6042): pid=3736 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=614 res=1
type=USER_START msg=audit(1695723601.860:6043): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1695723601.861:6044): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1695723601.934:6045): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1695723601.941:6046): pid=3736 uid=0 auid=0 ses=614 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=SERVICE_START msg=audit(1695723949.076:6047): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(1695723949.076:6048): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=USER ACCT msg=audit(1695726602.022:6049): pid=3863 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_access,pam_unix,pam_localuser acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_ACQ msg=audit(1695726602.022:6050): pid=3863 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1695726602.025:6051): pid=3863 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=615 res=1
type=USER_START msg=audit(1695726602.134:6052): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1695726602.136:6053): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1695726602.210:6054): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1695726602.214:6055): pid=3863 uid=0 auid=0 ses=615 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr

```


Шаг 17



```
[root@adkekisheva ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive
,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@adkekisheva ~]# 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@adkekisheva ~]# █
```

Рис. 17: Список портов

Шаг 18



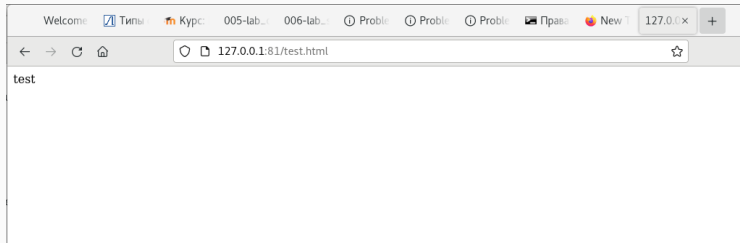


Рис. 18: перезапуск и изменение контекста

Шаг 19

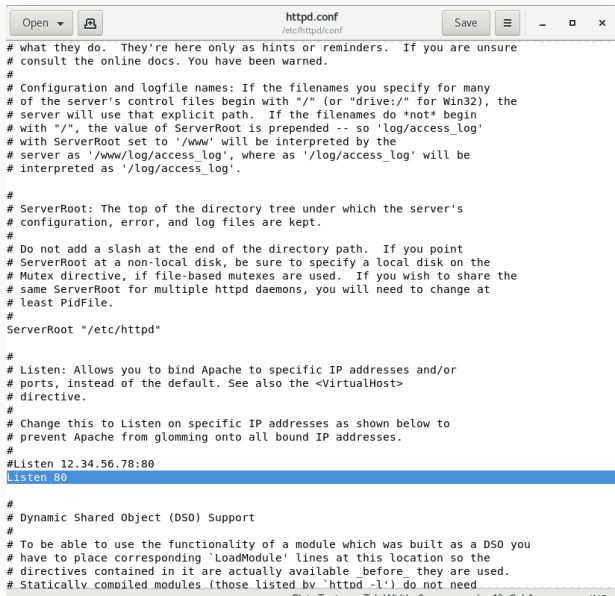




Рис. 19: Просмотр содержимого файла через браузер

Шаг 20





```

# what they do. They're here only as hints or reminders.  If you are unsure
# consult the online docs.  You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# 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 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
#
# 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

```


Шаг 21



```
[root@adkekisheva conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@adkekisheva conf]# cd
[root@adkekisheva ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@adkekisheva ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@adkekisheva ~]# cd /var/www/html
[root@adkekisheva html]# ls
```

Рис. 21: Удаление привязки к порту 81 и удаление файла

Выводы

1. Развила навыки администрирования ОС Linux.
2. Получила первое практическое знакомство с технологией SELinux1.
3. Проверила работу SELinx на практике совместно с веб-сервером Apache.