

Лабораторная работа №9

Управление SELinux

Перфилов Александр Константинович | группа НПИбд 03-24

Содержание

0.1	Цель работы:	4
0.2	Выполнение работы:	4
0.3	Посмотрим текущую информацию о состоянии SELinux:	5
0.4	Посмотрим, в каком режиме работает SELinux:	5
0.5	Изменим режим работы SELinux на разрешающий:	5
0.6	Откроем файл /etc/sysconfig/selinux в текстовом редакторе: . .	6
1	В открытом файле установим:	7
1.1	Сохраним изменения и перезагрузим систему:	8
1.2	После перезагрузки проверим статус SELinux:	8
1.3	Попробуем переключить режим работы:	9
1.4	Система сообщает, что SELinux отключён. Откроем файл /etc/sysconfig/selinux и установим:	10
1.5	Посмотрим контекст безопасности файла /etc/hosts:	11
1.6	Скопируем файл в домашний каталог и проверим контекст: . . .	12
1.7	Переместим файл обратно в /etc и снова проверим контекст: . .	13
1.8	Восстановим контекст безопасности:	13
1.9	Для массового исправления контекста выполним:	13
1.10	Установим необходимое ПО:	14
1.11	Создадим каталог и файл:	14
1.12	Откроем файл и добавим текст:	15
1.13	Запустим веб-сервер:	16
1.14	Откроем веб-страницу в браузере:	17
1.15	Применим новую метку контекста и восстановим контекст безопасности:	17
1.16	Ответы на контрольные вопросы:	18
1.17	Вывод:	19

Список иллюстраций

Список таблиц

0.1 Цель работы:

Целью данной работы является получение навыков работы с контекстом безопасности и политиками SELinux.

0.2 Выполнение работы:

0.2.1 Управление режимами SELinux:

Запустим терминал и получим полномочия администратора:

```
root@akppesfllov:~# sestatus -v
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

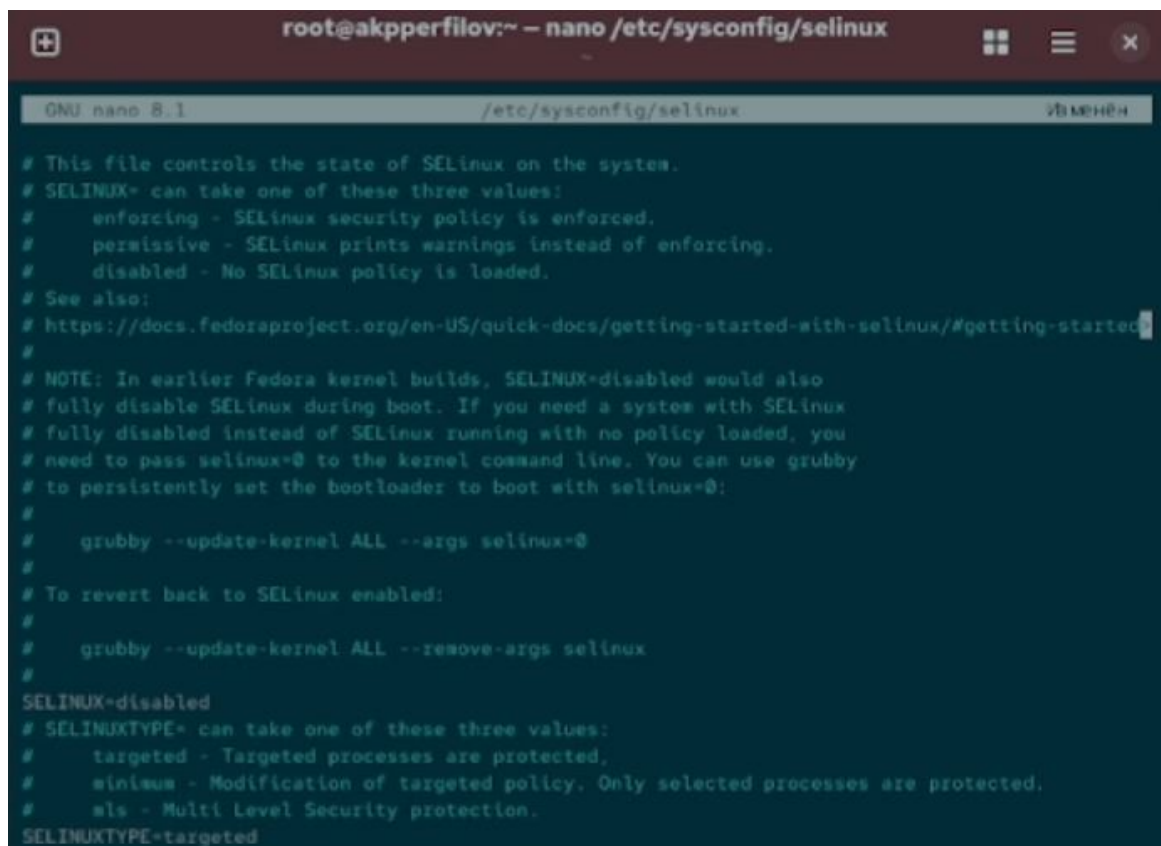
Process contexts:
Current context:                 unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                    system_u:object_r:passwd_file_t:s0
/etc/shadow                    system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                        system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                   system_u:object_r:getty_exec_t:s0
/sbin/init                    system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                 system_u:object_r:sshd_exec_t:s0
```

0.3 Посмотрим текущую информацию о состоянии SELinux:

```
root@akpperfilov:~# getenforce
Enforcing
root@akpperfilov:~# setenforce 0
root@akpperfilov:~# getenforce
Permissive
```

0.4 Посмотрим, в каком режиме работает SELinux:



```
root@akpperfilov:~ – nano /etc/sysconfig/selinux
GNU nano 8.1 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX* can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/#getting-started
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE* can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

0.5 Изменим режим работы SELinux на разрешающий:

```
root@akpperfilov:~# reboot
```

0.6 Откроем файл `/etc/sysconfig/selinux` в текстовом редакторе:

```
akpperfilov@akpperfilov:~$ su -  
Пароль:  
Последний вход в систему: Пт окт 31 15:48:35 MSK 2025 на pts/0  
root@akpperfilov:~# getenforce  
Disabled  
root@akpperfilov:~# setenforce 1  
setenforce: SELinux is disabled  
root@akpperfilov:~# nano /etc/sysconfig/selinux
```

Рис. 2. Просмотр режима работы SELinux, изменение режима работы и проверка, открытие файла в текстовом редакторе.

1 В открытом файле установим:

```
root@akpperfilov:~ – nano /etc/sysconfig/selinux
GNU nano 8.1 /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
#
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

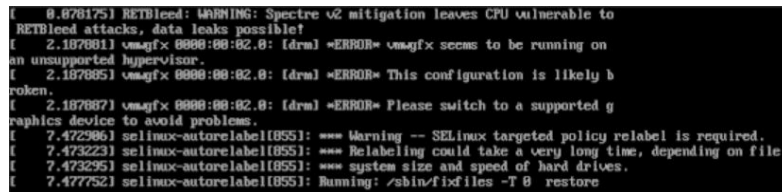
1.1 Сохраним изменения и перезагрузим систему:



```
root@akpperfilov:~# reboot
```

Рис.3. Установка в файле `SELINUX=disabled`, сохранение изменений и перезагрузка системы.

1.2 После перезагрузки проверим статус SELinux:



```
[ 0.070175] RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to  
RETbleed attacks, data leaks possible!  
[ 2.107081] vmgfx 0000:00:02.0: [drm] *ERROR* vmgfx seems to be running on  
an unsupported hypervisor.  
[ 2.107085] vmgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 2.107087] vmgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 7.472906] selinux-autorelabel(055): *** Warning -- SELinux targeted policy relabel is required.  
[ 7.473223] selinux-autorelabel(055): *** Relabeling could take a very long time, depending on file  
[ 7.473295] selinux-autorelabel(055): *** system size and speed of hard drives.  
[ 7.477752] selinux-autorelabel(055): Running: /sbin/fixfiles -T 0 restore
```


1.3 Попробуем переключить режим работы:

```
root@akpperfilov:~# sestatus -v
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          error (Success)
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                      system_u:object_r:shell_exec_t:s0
/bin/login                     system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object
_r:shell_exec_t:s0
/sbin/agetty                   system_u:object_r:getty_exec_t:s0
/sbin/init                     system_u:object_r:bin_t:s0 -> system_u:object
_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

1.4 Система сообщает, что SELinux отключён.

Откроем файл `/etc/sysconfig/selinux` и установим:

```
akpperfilov@akpperfilov:~$ su -
Пароль:
Последний вход в систему: Пт окт 31 16:02:28 MSK 2025 на pts/0
root@akpperfilov:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@akpperfilov:~# cp /etc/hosts ~/
root@akpperfilov:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@akpperfilov:~# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
root@akpperfilov:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@akpperfilov:~# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_conf_t:s0
root@akpperfilov:~# restorecon -v /etc/hosts
root@akpperfilov:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@akpperfilov:~# touch /.autorelabel
root@akpperfilov:~# reboot
```

Сохраним изменения и перезагрузим систему.

1.4.1 Использование restorecon для восстановления контекста безопасности:

1.5 Просмотрим контекст безопасности файла /etc/hosts:

```
[ OK ] Stopped fwupd.service - Firmware update daemon.
[ OK ] Stopped tuned.service - Dynamic System Tuning Daemon.
[ OK ] Stopped rsyslog.service - System Logging Service.
[ OK ] Stopped target network-online.target - Network is Online.
[ OK ] Stopped NetworkManager-wait-online.service - Network Manager Wait Online.
[ OK ] Started plymouth-reboot.service - Show Plymouth Reboot Screen.
NETSled: WARNING: Spectre v2 mitigation leaves CPU vulnerable to NETSled attacks, data leaks possible!
acpi PNP0A03:00: fail to add MRCONFIG information, can't access extended configuration space under this bridge
device-mapper: core: CONFIG_IMA_DISABLE_HTABLE is disabled. Duplicate IMA measurements will not be recorded in the IMA log.
vmwgfx 0000:00:02.0: [drm] "ERROR" vmwgfx seems to be running on an unsupported hypervisor.
vmwgfx 0000:00:02.0: [drm] "ERROR" This configuration is likely broken.
vmwgfx 0000:00:02.0: [drm] "ERROR" Please switch to a supported graphics device to avoid problems.
Warning: Unmaintained driver is detected: atombios
clocksource: Long readout interval, skipping watchdog check: cs_nsec: 1043473583 wd_nsec: 1043473215
Warning: Unmaintained driver is detected: ip_set
block dm-0: the capability attribute has been deprecated.
[ OK ] Stopped session-2.scope - Session 2 of User akperfilov.
Stopping user@1000.service - User Manager for UID 1000...
[ OK ] Stopped user@1000.service - User Manager for UID 1000.
Stopping systemd-user-sessions.service - Permit User Sessions...
Stopping user-runtime-dir@1000.service - User Runtime Directory /run/user/1000...
[ OK ] Stopped dracut-shutdown.service - Restore /run/initramfs on shutdown.
Starting plymouth-switch-root-initramfs.service - Tell Plymouth To Jump To initramfs...
[ OK ] Unmounted run-user-1000.mount - /run/user/1000.
[ OK ] Stopped systemd-user-sessions.service - Permit User Sessions.
[ OK ] Stopped user-runtime-dir@1000.service - User Runtime Directory /run/user/1000.
[ OK ] Removed slice user-1000.slice - User Slice of UID 1000.
[ OK ] Finished plymouth-switch-root-initramfs.service - Tell Plymouth To Jump To initramfs.
[ OK ] Stopped httpd.service - The Apache HTTP Server.
[ OK ] Stopped target network.target - Network.
[ OK ] Stopped target remote-fs.target - Remote File Systems.
Stopping NetworkManager.service - Network Manager...
Stopping wpa_supplicant.service - WPA supplicant...
[ OK ] Stopped wpa_supplicant.service - WPA supplicant.
[ OK ] Stopped NetworkManager.service - Network Manager.
[ OK ] Stopped target network-pre.target - Preparation for Network.
Stopping firewallld.service - firewallld - dynamic firewall daemon...
[ OK ] Stopped systemd-network-generator.service - Generate network units from Kernel command line.
[ OK ] Stopped firewallld.service - firewallld - dynamic firewall daemon.
Stopping polkit.service - Authorization Manager...
[ OK ] Stopped polkit.service - Authorization Manager.
```

1.6 Скопируем файл в домашний каталог и проверим контекст:

```
root@akpperfilov:~# dnf -y install httpd
Extra Packages for Enterprise Linux 10 - x86_64 83 kB/s | 37 kB      00:00
Extra Packages for Enterprise Linux 10 - x86_64 5.3 MB/s | 4.8 MB    00:00
R Tools PPA                               166 B/s | 1.5 kB      00:09
R Tools PPA                               15 kB/s | 41 kB       00:02
Rocky Linux 10 - BaseOS                   12 kB/s | 4.3 kB     00:00
Rocky Linux 10 - BaseOS                   18 MB/s | 22 MB      00:01
Rocky Linux 10 - AppStream                 16 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                2.3 MB/s | 2.2 MB    00:00
Rocky Linux 10 - Extras                   11 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                   11 kB/s | 5.5 kB     00:00
Пакет httpd-2.4.63-1.el10_0.2.x86_64 уже установлен.
Зависимости разрешены.
Нет действий для выполнения.
Выполнено!
root@akpperfilov:~# dnf -y install lynx
Последняя проверка окончания срока действия метаданных: 0:00:14 назад, Пт 31
окт 2025 16:11:58.
Зависимости разрешены.
=====
Пакет      Архитектура  Версия      Репозиторий    Размер
=====
Установка:
  lynx      x86_64      2.9.0-6.el10  appstream      1.6 М
Результат транзакции
=====
Установка 1 Пакет

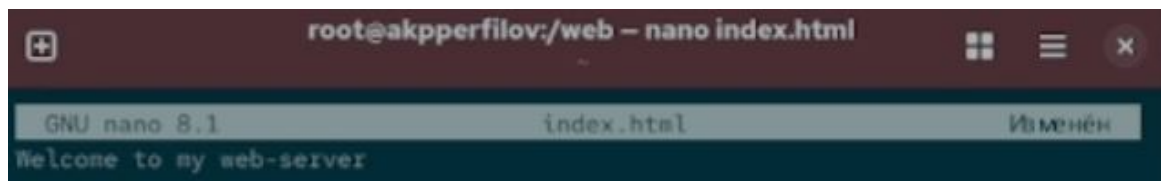
Объем загрузки: 1.6 М
Объем изменений: 6.0 М
Загрузка пакетов:
lynx-2.9.0-6.el10.x  0% [          ] --- B/s | 0 В  --:-- ETA
```

1.7 Переместим файл обратно в /etc и снова

проверим контекст:

```
root@akpperfilov:~# mkdir /web
root@akpperfilov:~# cd /web
root@akpperfilov:/web# touch index.html
root@akpperfilov:/web# nano index.html
```

1.8 Восстановим контекст безопасности:



1.9 Для массового исправления контекста выполним:

```
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
#<Directory "/var/www">
#   AllowOverride None
#   # Allow open access:
#   Require all granted
#</Directory>
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
```

1.9.1 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера:

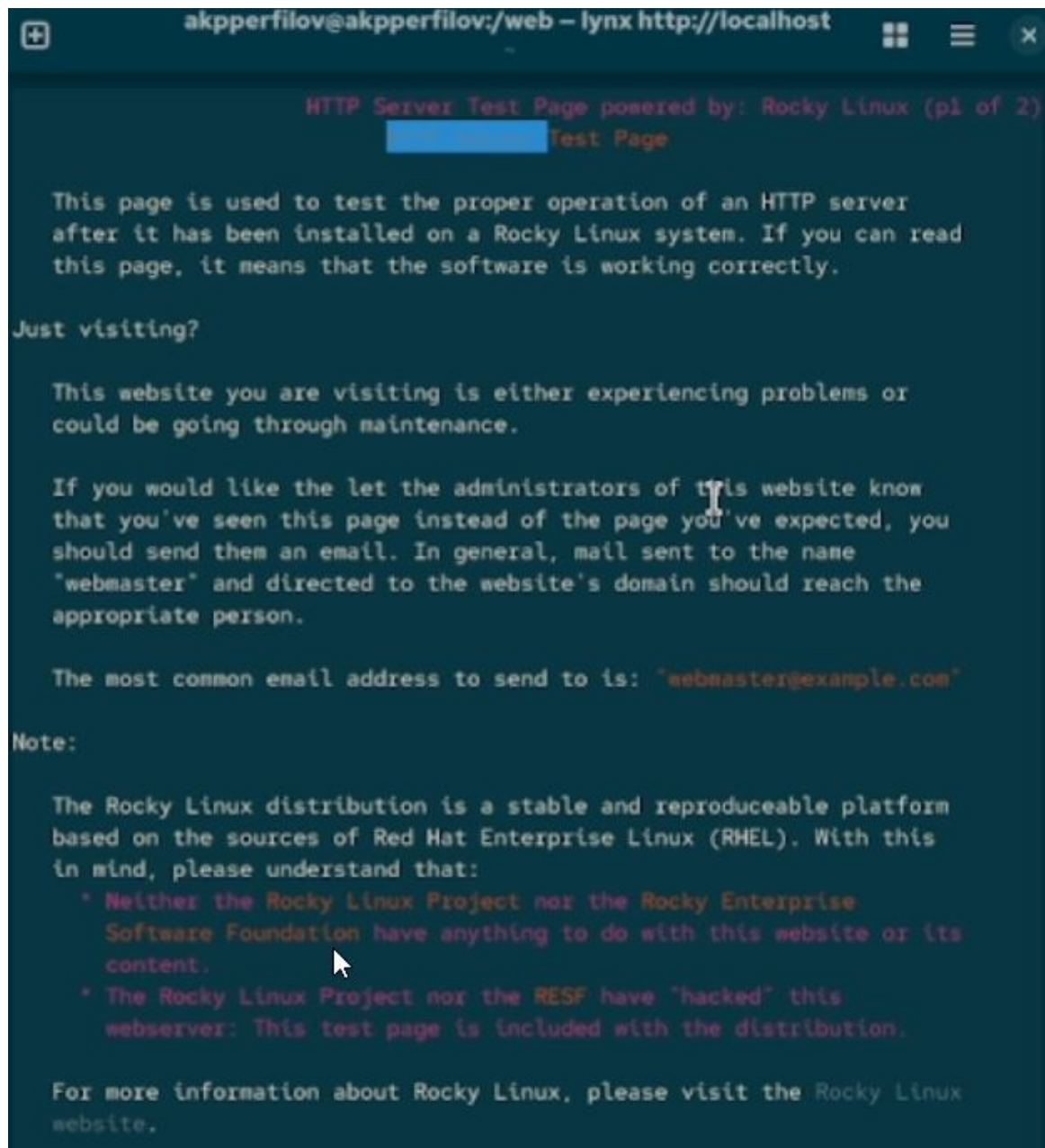
1.10 Установим необходимое ПО:

```
root@akpperfilov:/web# systemctl start httpd  
root@akpperfilov:/web# systemctl enable httpd
```

1.11 Создадим каталог и файл:

```
root@akpperfilov:/web# su akpperfilov  
akpperfilov@akpperfilov:/web$ lynx http://localhost
```


1.12 Откроем файл и добавим текст:



```
akpperfilov@akpperfilov:/web - lynx http://localhost
HTTP Server Test Page powered by: Rocky Linux (p1 of 2)
Test Page

This page is used to test the proper operation of an HTTP server
after it has been installed on a Rocky Linux system. If you can read
this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or
could be going through maintenance.

If you would like the let the administrators of this website know
that you've seen this page instead of the page you've expected, you
should send them an email. In general, mail sent to the name
"webmaster" and directed to the website's domain should reach the
appropriate person.

The most common email address to send to is: "webmaster@example.com"

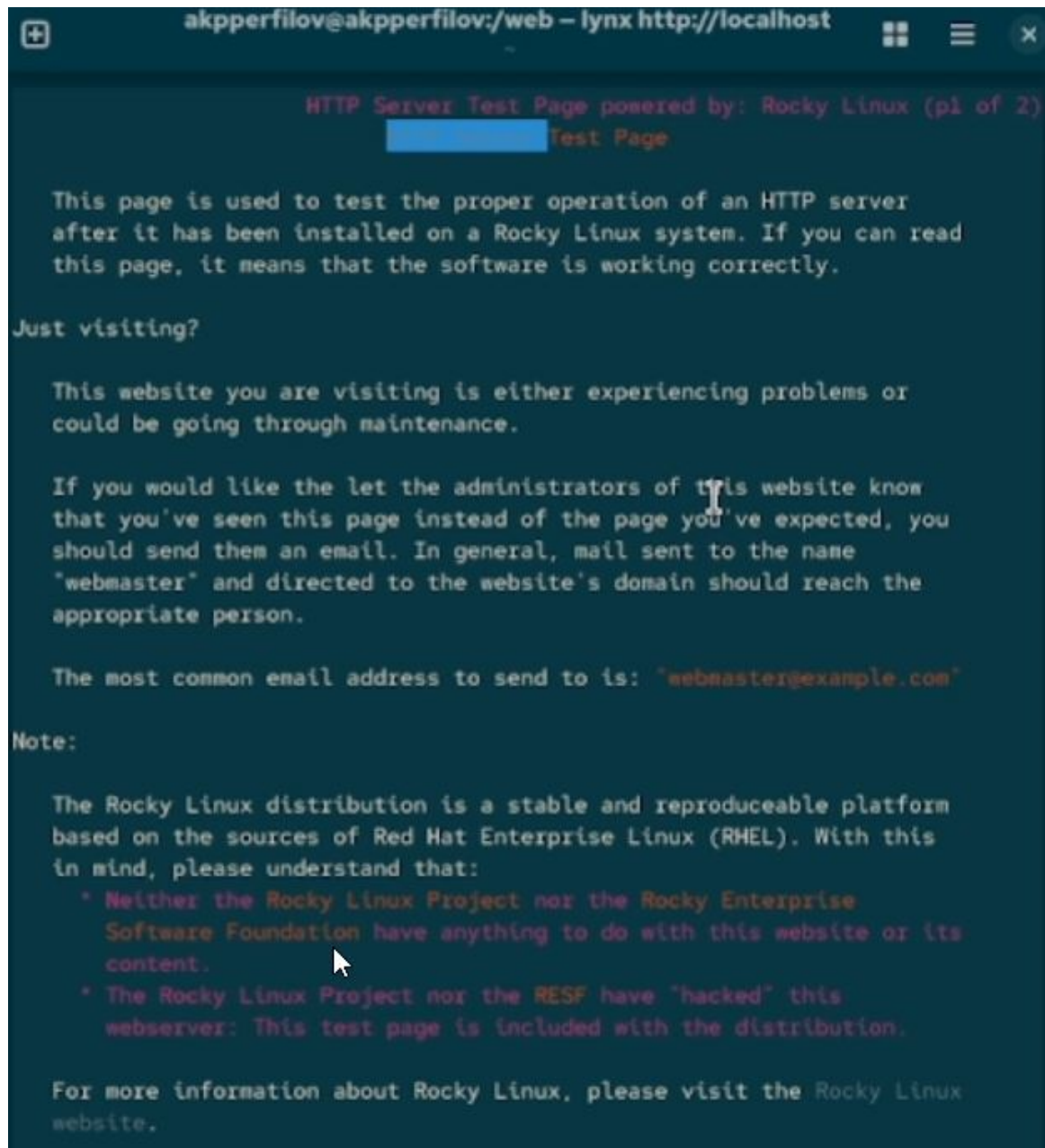
Note:

The Rocky Linux distribution is a stable and reproduceable platform
based on the sources of Red Hat Enterprise Linux (RHEL). With this
in mind, please understand that:
* Neither the Rocky Linux Project nor the Rocky Enterprise
  Software Foundation have anything to do with this website or its
  content.
* The Rocky Linux Project nor the RESF have "hacked" this
  webserver: This test page is included with the distribution.

For more information about Rocky Linux, please visit the Rocky Linux
website.
```

Изменим файл конфигурации Apache `/etc/httpd/conf/httpd.conf`, заменив `DocumentRoot "/var/www/html"` на `DocumentRoot "/web"`. Также обновим настройки доступа.

1.13 Запустим веб-сервер:



The screenshot shows a terminal window with a Lynx web browser interface. The title bar reads 'akpperfilov@akpperfilov:/web - lynx http://localhost'. The main content area displays the 'HTTP Server Test Page powered by: Rocky Linux (p1 of 2)'. The page text explains its purpose for testing HTTP server operation on Rocky Linux and provides instructions for reporting issues via email to 'webmaster@example.com'. It also includes a note about the Rocky Linux distribution's stability and a disclaimer from the Rocky Linux Project and RESF. The page concludes with a link to the Rocky Linux website.

```
akpperfilov@akpperfilov:/web - lynx http://localhost
HTTP Server Test Page powered by: Rocky Linux (p1 of 2)
Test Page

This page is used to test the proper operation of an HTTP server
after it has been installed on a Rocky Linux system. If you can read
this page, it means that the software is working correctly.

Just visiting?

This website you are visiting is either experiencing problems or
could be going through maintenance.

If you would like to let the administrators of this website know
that you've seen this page instead of the page you've expected, you
should send them an email. In general, mail sent to the name
"webmaster" and directed to the website's domain should reach the
appropriate person.

The most common email address to send to is: "webmaster@example.com"

Note:

The Rocky Linux distribution is a stable and reproduceable platform
based on the sources of Red Hat Enterprise Linux (RHEL). With this
in mind, please understand that:
* Neither the Rocky Linux Project nor the Rocky Enterprise
  Software Foundation have anything to do with this website or its
  content.
* The Rocky Linux Project nor the RESF have "hacked" this
  webserver: This test page is included with the distribution.

For more information about Rocky Linux, please visit the Rocky Linux
website.
```


1.14 Откроем веб-страницу в браузере:

```
root@akpperfilov:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@akpperfilov:~# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
```

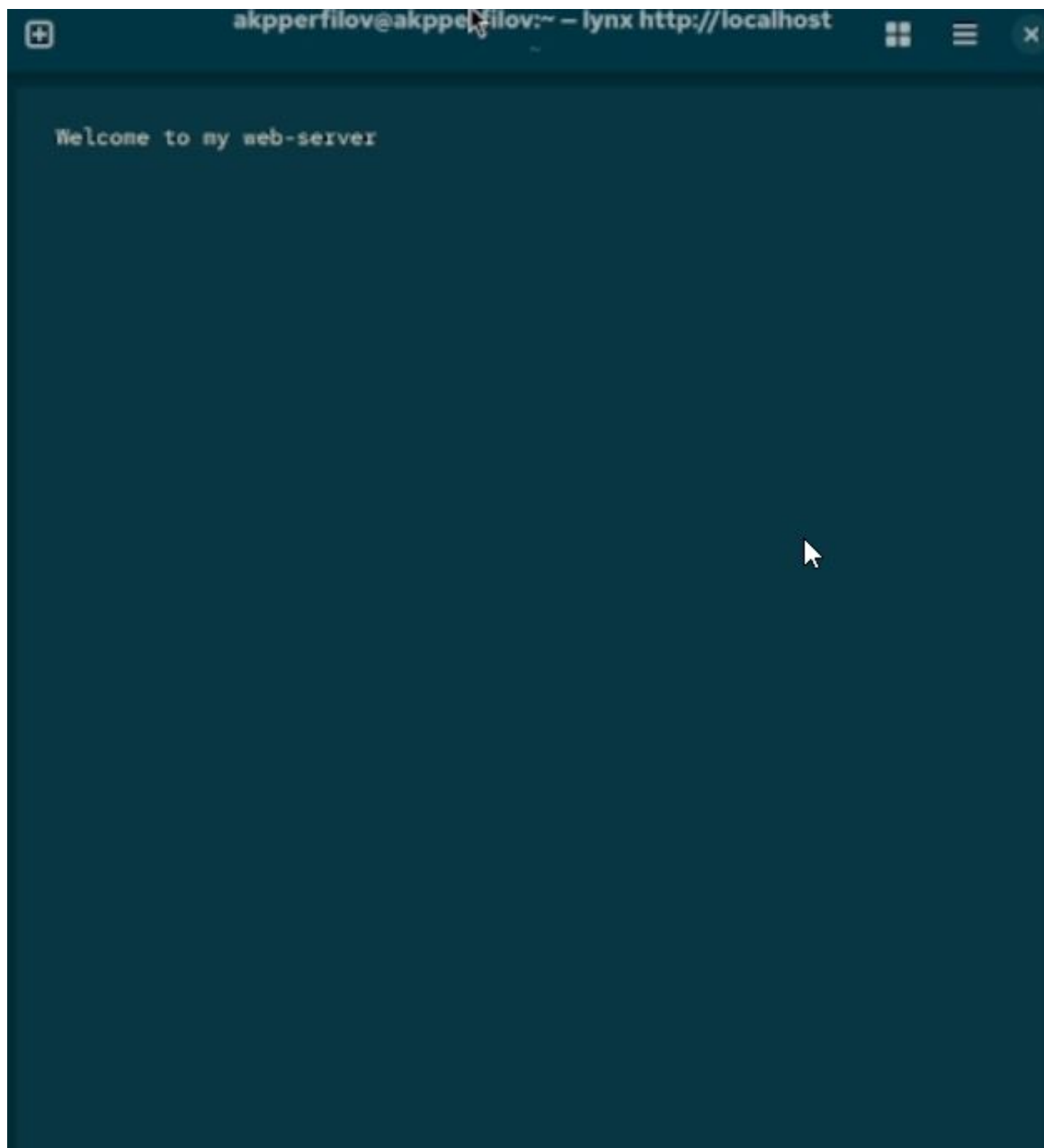
1.15 Применим новую метку контекста и восстановим контекст безопасности:

```
akpperfilov@akpperfilov:~$ lynx http://localhost
```

Рис. 19. Настройка контекста безопасности для веб-сервера.

1.15.1 Работа с переключателями SELinux:

Посмотрим список переключателей SELinux для службы ftp. Изменим значение переключателя. Изменим постоянное значение переключателя:



1.16 Ответы на контрольные вопросы:

1. setenforce 0
2. getsebool -a

3. `audit2allow`
 4. `bash semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?" re-storecon -R -v /web`
 5. `/etc/sysconfig/selinux`
 6. `/var/log/audit/audit.log`
 7. `getsebool -a | grep ftp`
 8. `ps -eZ` или `id -Z`
-

1.17 Вывод:

В ходе выполнения лабораторной работы были получены навыки работы с контекстом безопасности и политиками