

Отчет по выполнению лабораторной работы

Лабораторная работа №9

Полина Витальевна Барабаш

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Ответы на контрольные вопросы	20
4	Выводы	22

Список иллюстраций

2.1	Переход в режим суперпользователя	6
2.2	Проверка текущей информации о состоянии SELinux	7
2.3	Просмотр режима работы SELinux	8
2.4	Изменение режима работы и проверка	8
2.5	Изменение настроек в файле	8
2.6	Проверка статуса после изменения настроек в файле	9
2.7	Попытка переключить режим работы SELinux	9
2.8	Обратное изменение настроек в файле	10
2.9	Повторная проверка статуса SELinux	10
2.10	Просмотр контекста безопасности файла	11
2.11	Проверка контекста безопасности скопированного файла	11
2.12	Перемещение скопированного файла в исходную папку	11
2.13	Проверка метки контекста перемещенного файла	12
2.14	Исправление контекста безопасности	12
2.15	Проверка изменений типа контекста безопасности	12
2.16	Создание файла .autorelabel	13
2.17	Установка httpd	13
2.18	Установка lynx	14
2.19	Создание каталога и файла	14
2.20	Добавление нужной фразы в файл	14
2.21	Комментирование и добавление строк	15
2.22	Комментирование и добавление разделов	15
2.23	Запуск веб-сервера и службы httpd	16
2.24	Запуск веб-сервера в текстовом браузере	16
2.25	Применение новой метки контекста к /web и восстановление кон- текста безопасности	17
2.26	Повторное открытие веб-сервера в текстовом браузере	17
2.27	Просмотр списка переключателей SELinux для службы ftp	18
2.28	Просмотр списка переключателей с пояснением	18
2.29	Изменение переключателя для службы и проверка изменения . . .	19
2.30	Просмотр списка переключателей с пояснением	19
2.31	Изменение постоянного значения переключателя для службы и просмотр списка переключателей	19

List of Tables

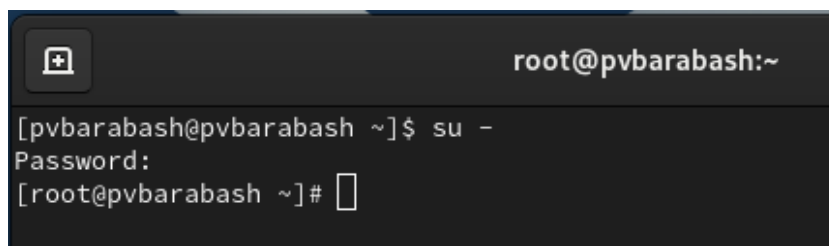
1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Выполнение лабораторной работы

Задание 1. Получите полномочия администратора.

Я перешла в режим работы суперпользователя, используя команду `su -` (рис. 2.1).

A screenshot of a terminal window with a dark background. The title bar at the top shows a window icon on the left and the text 'root@pvbarabash:~' on the right. The terminal content shows the following sequence: a prompt '[pvbarabash@pvbarabash ~]\$' followed by the command 'su -', then the prompt 'Password:' with an empty space for input, and finally the root prompt '[root@pvbarabash ~]#' with a cursor. The text is white on a dark background.

```
[pvbarabash@pvbarabash ~]$ su -  
Password:  
[root@pvbarabash ~]#
```

Рис. 2.1: Переход в режим суперпользователя

Задание 2. Просмотрите текущую информацию о состоянии SELinux.

Я ввела команду `sestatus -v`, чтобы посмотреть текущую информацию о состоянии SELinux (рис. 2.2).

```

[root@pvbarabash ~]# 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
0
/usr/sbin/sshd                system_u:object_r:sshd_exec_t:s0
[root@pvbarabash ~]#

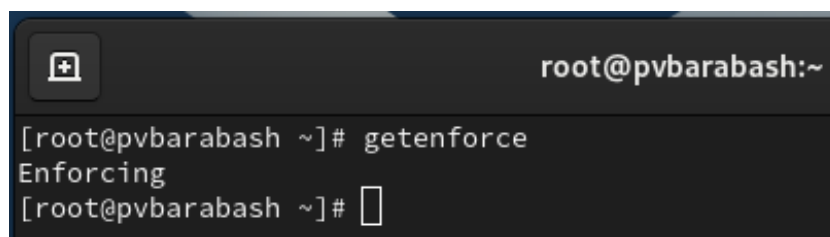
```

Рис. 2.2: Проверка текущей информации о состоянии SELinux

SELinux status: показывает, включен ли SELinux. Значение может быть “enabled” (включен) или “disabled” (выключен). **SELinux mount:** указывает, где смонтирована файловая система SELinux. **SELinux root directory:** путь к корневому каталогу конфигурации SELinux. **Loaded policy name:** название загруженной политики безопасности. **Current mode:** текущий режим работы SELinux. В данном случае “enforcing”, что означает, что политики SELinux применяются. Также могут быть значения “permissive” и “disabled”. **Mode from config file:** режим, указанных в конфигурационном файле SELinux. Это значение может совпадать с текущим режимом или отличаться. **Policy MLS status:** статус поддержки многоуровневой безопасности (MLS). Может быть “enabled” или “disabled”. **Policy deny_unknown status:** указывает, разрешено ли отклонение неизвестных типов объектов. Значение может быть “allowed” или “denied”. **Max kernel policy version:** максимальная версия политики ядра, которая поддерживается системой.

Задание 3. Посмотрите, в каком режиме работает SELinux.

Я использовала команду `getenforce`, чтобы посмотреть, в каком режиме работает SELinux (рис. 2.3).

A terminal window with a dark background. The prompt is root@pvbarabash:~. The command 'getenforce' has been entered, and the output is 'Enforcing'.

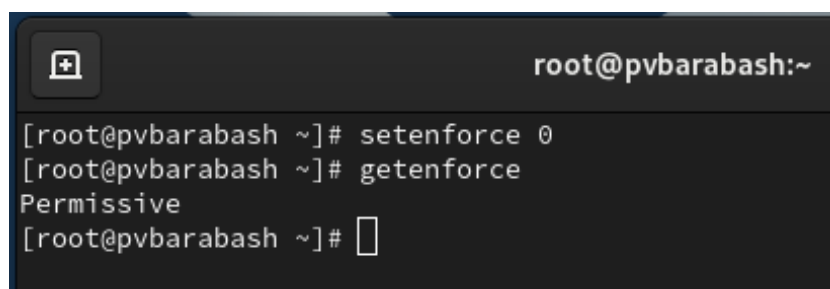
```
root@pvbarabash:~  
[root@pvbarabash ~]# getenforce  
Enforcing  
[root@pvbarabash ~]#
```

Рис. 2.3: Просмотр режима работы SELinux

Как можно видеть на скриншоте, SELinux находится в режиме принудительного исполнения (Enforcing).

Задание 4. Измените режим работы SELinux на разрешающий (Permissive) и снова проверьте, в каком режиме работает SELinux.

Я изменила режим работы SELinux на разрешающий с помощью команды `setenforce 0` и снова ввела команду `getenforce` (рис. 2.4).

A terminal window with a dark background. The prompt is root@pvbarabash:~. The command 'setenforce 0' has been entered. Then 'getenforce' has been entered, and the output is 'Permissive'.

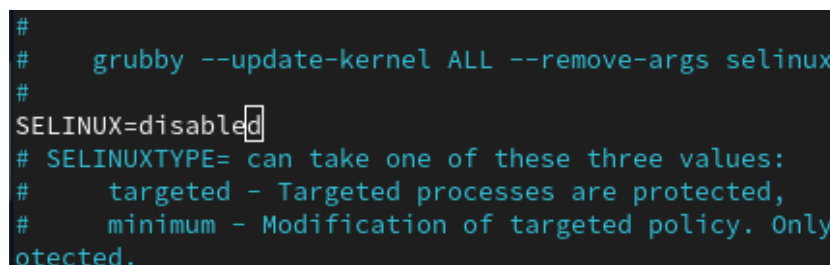
```
root@pvbarabash:~  
[root@pvbarabash ~]# setenforce 0  
[root@pvbarabash ~]# getenforce  
Permissive  
[root@pvbarabash ~]#
```

Рис. 2.4: Изменение режима работы и проверка

Как можно видеть, режим работы действительно изменился на необходимый.

Задание 5. В файле `/etc/sysconfig/selinux` с помощью редактора установите `SELINUX=disabled`. Перезагрузите систему.

Я использовала редактор `vim`, чтобы изменить файл (рис. 2.5).

A screenshot of a text file, likely /etc/sysconfig/selinux, with a dark background. The file contains several lines of text, including comments about grubby and SELINUXTYPE, and the line 'SELINUX=disabled' which is currently being edited with a cursor at the end.

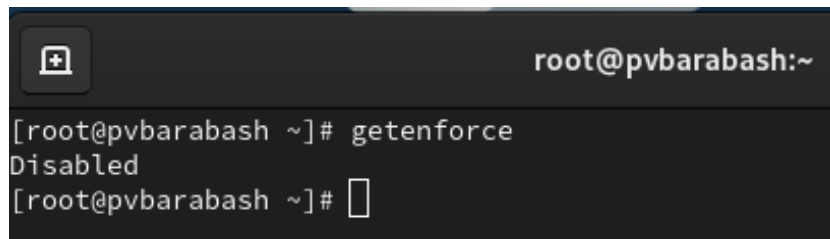
```
#  
# grubby --update-kernel ALL --remove-args selinux  
#  
SELINUX=disabled  
# SELINUXTYPE= can take one of these three values:  
#   targeted - Targeted processes are protected,  
#   minimum - Modification of targeted policy. Only  
#   otected.
```

Рис. 2.5: Изменение настроек в файле

Затем я перезапустила систему с помощью команды `reboot`.

Задание 6. После перезагрузки запустите терминал и получите полномочия администратора. Посмотрите статус SELinux.

После перезагрузки я запустила терминал и получила полномочия администратора. Затем я посмотрела статус SELinux с помощью всё той же команды `getenforce` (рис. 2.6).

A terminal window with a dark background. The title bar shows a window icon and the text 'root@pvbarabash:~'. The terminal content shows the command '[root@pvbarabash ~]# getenforce' followed by the output 'Disabled'. The prompt '[root@pvbarabash ~]#' is followed by a cursor.

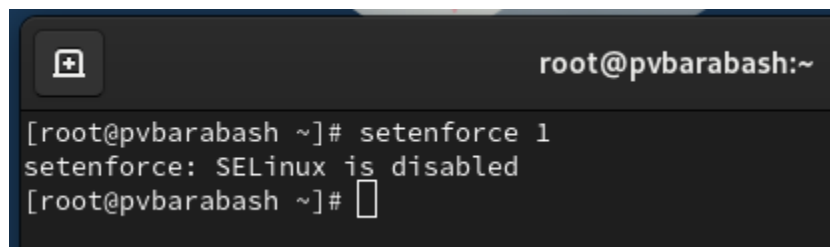
```
root@pvbarabash:~  
[root@pvbarabash ~]# getenforce  
Disabled  
[root@pvbarabash ~]#
```

Рис. 2.6: Проверка статуса после изменения настроек в файле

Действительно, статус изменен на `disabled`.

Задание 7. Попробуйте переключить режим работы SELinux.

Я использовала команду `setenforce 1`, но получила сообщение, что SELinux is disabled (рис. 2.7).

A terminal window with a dark background. The title bar shows a window icon and the text 'root@pvbarabash:~'. The terminal content shows the command '[root@pvbarabash ~]# setenforce 1' followed by the output 'setenforce: SELinux is disabled'. The prompt '[root@pvbarabash ~]#' is followed by a cursor.

```
root@pvbarabash:~  
[root@pvbarabash ~]# setenforce 1  
setenforce: SELinux is disabled  
[root@pvbarabash ~]#
```

Рис. 2.7: Попытка переключить режим работы SELinux

Задание 8. Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите: `SELINUX=enforcing`. Перезагрузите систему.

Я снова открыла файл в редакторе `vim` и изменила настройки на `enforcing` (рис. 2.8).

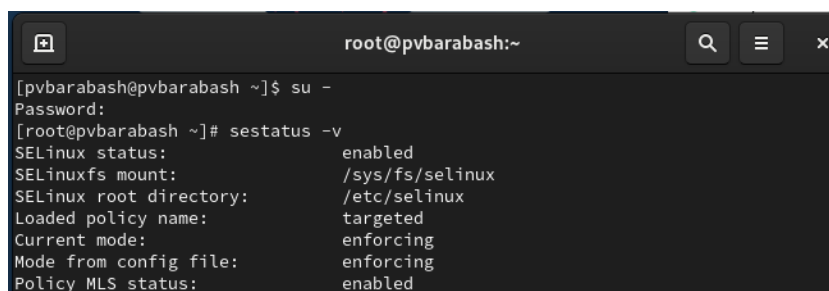
```
#
# grubby --update-kernel ALL --remove-args selinux
#
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only
#   tected.
#   ... Multi-level Security protection
```

Рис. 2.8: Обратное изменение настроек в файле

Затем я перезагрузила систему.

Задание 9. После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux.

Я снова получила полномочия администратора и посмотрела текущую информацию о состоянии SELinux с помощью команды `sestatus -v` (рис. 2.9).



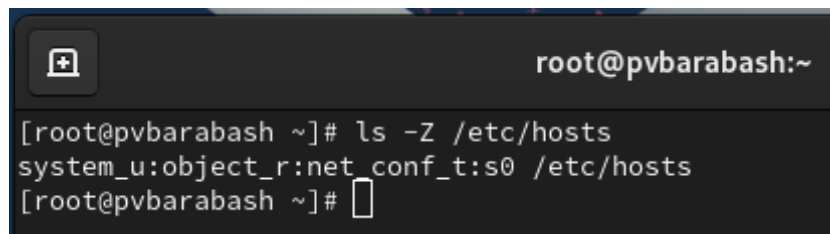
```
root@pvbarabash:~
[pvbarabash@pvbarabash ~]$ su -
Password:
[root@pvbarabash ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
```

Рис. 2.9: Повторная проверка статуса SELinux

Я убедилась, что система работает в принудительном режиме (enforcing) использования SELinux.

Задание 10. Запустите терминал и получите полномочия администратора. Посмотрите контекст безопасности файла `/etc/hosts`.

Я использовала команду `ls -Z /etc/hosts` и увидела, что у файла есть метка контекста `net_conf_t` (рис. 2.10).

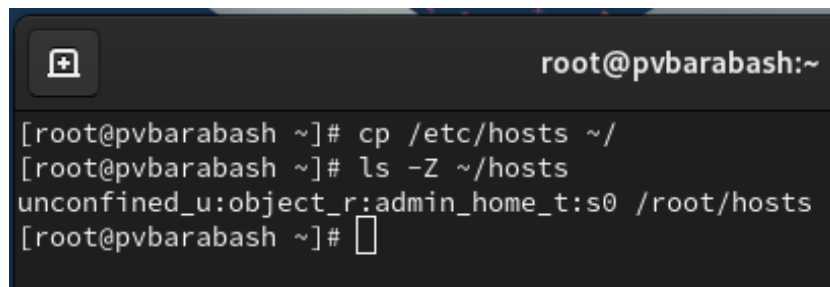


```
root@pvbarabash:~  
[root@pvbarabash ~]# ls -Z /etc/hosts  
system_u:object_r:net_conf_t:s0 /etc/hosts  
[root@pvbarabash ~]#
```

Рис. 2.10: Просмотр контекста безопасности файла

Задание 11. Скопируйте файл `/etc/hosts` в домашний каталог. Проверьте контекст файла `~/hosts`

Я скопировала файл `/etc/hosts` в домашний каталог с помощью команды `cp`. Затем я проверила контекст скопированного файла (рис. 2.11).



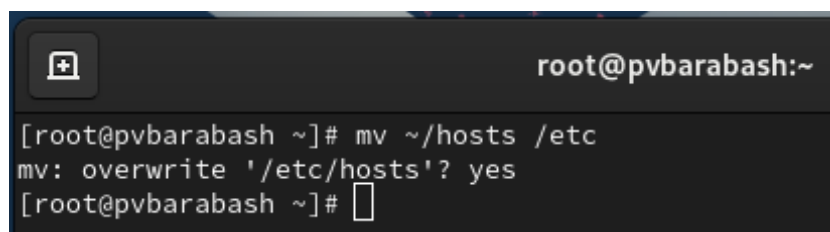
```
root@pvbarabash:~  
[root@pvbarabash ~]# cp /etc/hosts ~/  
[root@pvbarabash ~]# ls -Z ~/hosts  
unconfined_u:object_r:admin_home_t:s0 /root/hosts  
[root@pvbarabash ~]#
```

Рис. 2.11: Проверка контекста безопасности скопированного файла

Как можно видеть, у этого файла метка контекста стала `admin_home_t`.

Задание 12. Попробуйте перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`. И подтвердите, что вы хотите сделать это.

Я использовала команду `mv ~/hosts /etc` и подтвердила, что хочу переместить файл (рис. 2.12).

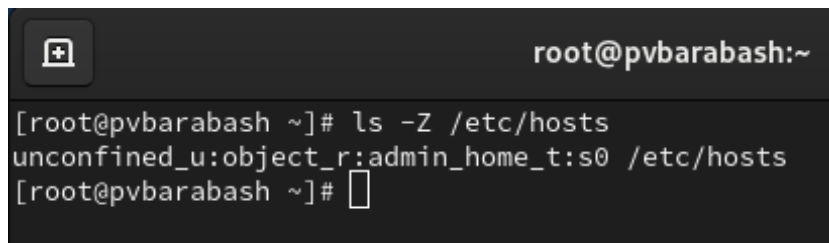


```
root@pvbarabash:~  
[root@pvbarabash ~]# mv ~/hosts /etc  
mv: overwrite '/etc/hosts'? yes  
[root@pvbarabash ~]#
```

Рис. 2.12: Перемещение скопированного файла в исходную папку

Задание 13. Убедитесь, что тип контекста по-прежнему установлен на `admin_home_t`.

Я использовала команды `ls -Z /etc/hosts` и убедилась, что тип контекста по-прежнему установлен на `admin_home_t` (рис. 2.13).

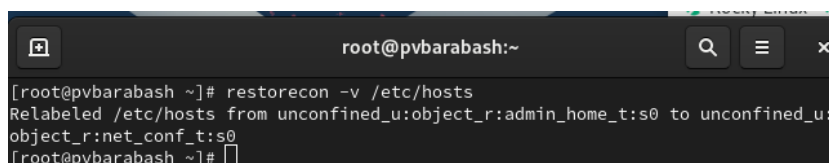


```
root@pvbarabash:~  
[root@pvbarabash ~]# ls -Z /etc/hosts  
unconfined_u:object_r:admin_home_t:s0 /etc/hosts  
[root@pvbarabash ~]#
```

Рис. 2.13: Проверка метки контекста перемещенного файла

Задание 14. Исправьте контекст безопасности.

Я выполнила команду `restorecon -v /etc/hosts`, чтобы исправить контекст безопасности (рис. 2.14).



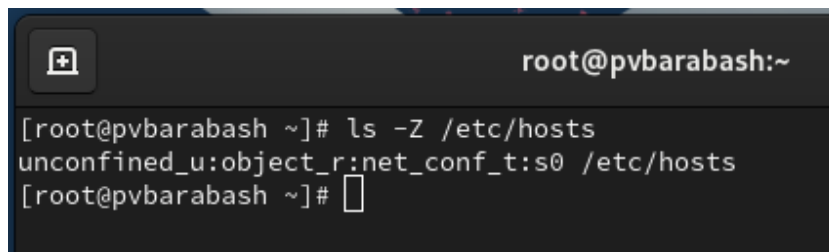
```
root@pvbarabash:~  
[root@pvbarabash ~]# restorecon -v /etc/hosts  
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:  
object_r:net_conf_t:s0  
[root@pvbarabash ~]#
```

Рис. 2.14: Исправление контекста безопасности

Благодаря опции `-v`, мы получили сообщение об исправлении.

Задание 15. Убедитесь, что тип контекста изменился.

Я вновь ввела команду `ls -Z /etc/hosts` и убедилась, что тип контекста изменился (рис. 2.15).

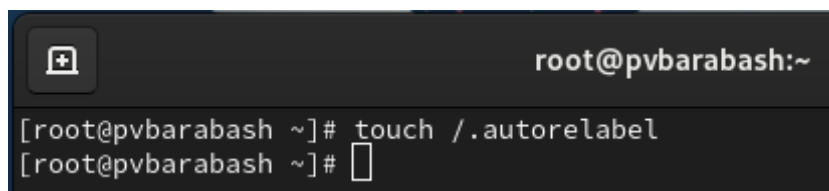


```
root@pvbarabash:~  
[root@pvbarabash ~]# ls -Z /etc/hosts  
unconfined_u:object_r:net_conf_t:s0 /etc/hosts  
[root@pvbarabash ~]#
```

Рис. 2.15: Проверка изменений типа контекста безопасности

Задание 16. Для массового исправления контекста безопасности на файловой системе введите `touch /.autorelabel` и перезагрузите систему. Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения. Вы увидите, что файловая система автоматически перемаркирована.

Я ввела приведенную команду (рис. 2.16).



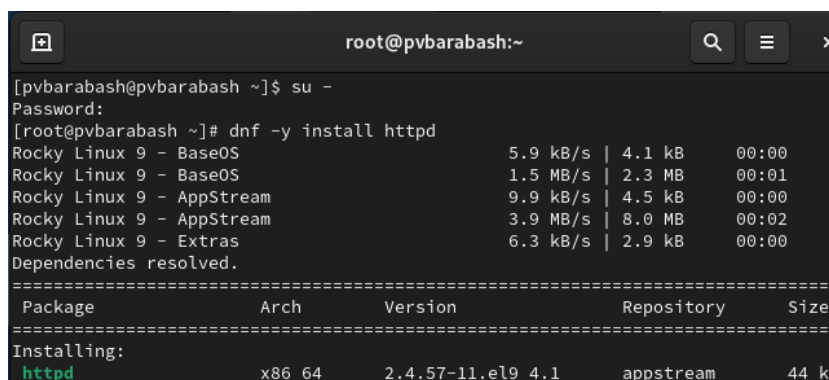
```
root@pvbarabash:~  
[root@pvbarabash ~]# touch /.autorelabel  
[root@pvbarabash ~]#
```

Рис. 2.16: Создание файла `.autorelabel`

Затем перезапустила систему. И при перезагрузке нажала Esc и действительно увидела, что файловая система перемаркировалась.

Задание 17. Получите права администратора. Установите необходимое программное обеспечение: `dnf -y install httpd` и `dnf -y install lynx`.

Я получила права администратора, а затем использовала обе приведенные команды, чтобы установить необходимое ПО (рис. 2.17) и (рис. 2.18).



```
[pvbarabash@pvbarabash ~]$ su -  
Password:  
[root@pvbarabash ~]# dnf -y install httpd  
Rocky Linux 9 - BaseOS                    5.9 kB/s | 4.1 kB    00:00  
Rocky Linux 9 - BaseOS                    1.5 MB/s | 2.3 MB    00:01  
Rocky Linux 9 - AppStream                 9.9 kB/s | 4.5 kB    00:00  
Rocky Linux 9 - AppStream                 3.9 MB/s | 8.0 MB    00:02  
Rocky Linux 9 - Extras                    6.3 kB/s | 2.9 kB    00:00  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
httpd	x86_64	2.4.57-11.el9_4.1	appstream	44 k

Рис. 2.17: Установка `httpd`

```
[root@pvbarabash ~]# dnf -y install lynx
Last metadata expiration check: 0:00:51 ago on Mon 28 Oct 2024 04:18:24 PM MSK.
Dependencies resolved.
=====
Package           Architecture Version           Repository        Size
=====
Installing:
lynx              x86_64         2.8.9-20.el9     appstream         1.5 M
```

Рис. 2.18: Установка lynx

Задание 18. Создайте новое хранилище для файлов web-сервера. Создайте файл index.html в каталоге с контентом веб-сервера.

Я создала каталог /web с помощью команды mkdir. Затем перешла в этот каталог с помощью команды cd и создала внутри файл index.html с помощью команды touch (рис. 2.19).

```
root@pvbarabash:/web

[root@pvbarabash ~]# mkdir /web
[root@pvbarabash ~]# cd /web
[root@pvbarabash web]# touch index.html
[root@pvbarabash web]#
```

Рис. 2.19: Создание каталога и файла

Задание 19. Поместите в файл следующий текст: Welcome to my web-server. Я открыла файл index.html в vim и добавила туда нужную фразу (рис. 2.20).

```
root@pvbarabash:/web

Welcome to my web-server
```

Рис. 2.20: Добавление нужной фразы в файл

Задание 20. В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot "/var/www/html" и ниже добавьте строку DocumentRoot "/web".

Я открыла файл /etc/httpd/conf/httpd.conf с помощью редактора vim, затем я закомментировала нужную строку и добавила данную (рис. 2.21)

```
# symbolic links and aliases may be used to
#
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
#
# Relax access to content within /var/www.
#
```

Рис. 2.21: Комментирование и добавление строк

Задание 21. Затем в этом же файле ниже закомментируйте раздел

<Directory "/var/www"> AllowOverride None Require all granted

и добавьте следующий раздел, определяющий правила доступа:

<Directory "/web"> AllowOverride None Require all granted

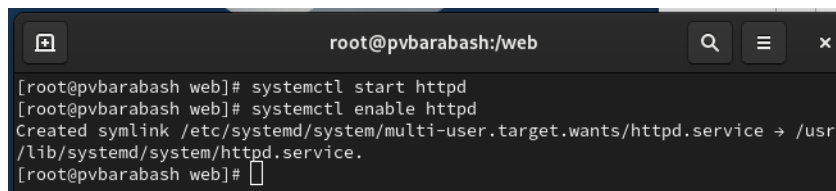
Все в том же открытом в vim файле я закомментировала нужный раздел и добавила данных (рис. 2.22).

```
#
#<Directory "/var/www">
#   AllowOverride None
#   # Allow open access:
#   # Require all granted
#</Directory>
<Directory "/web">
    AllowOverride None
    Require all granted
</Directory>
# Further relax access to the
```

Рис. 2.22: Комментирование и добавление разделов

Задание 22. Запустите веб-сервер и службу httpd.

Я использовала команды `systemctl start httpd` и `systemctl enable httpd`, чтобы запустить веб-сервер и службу httpd (рис. 2.23).

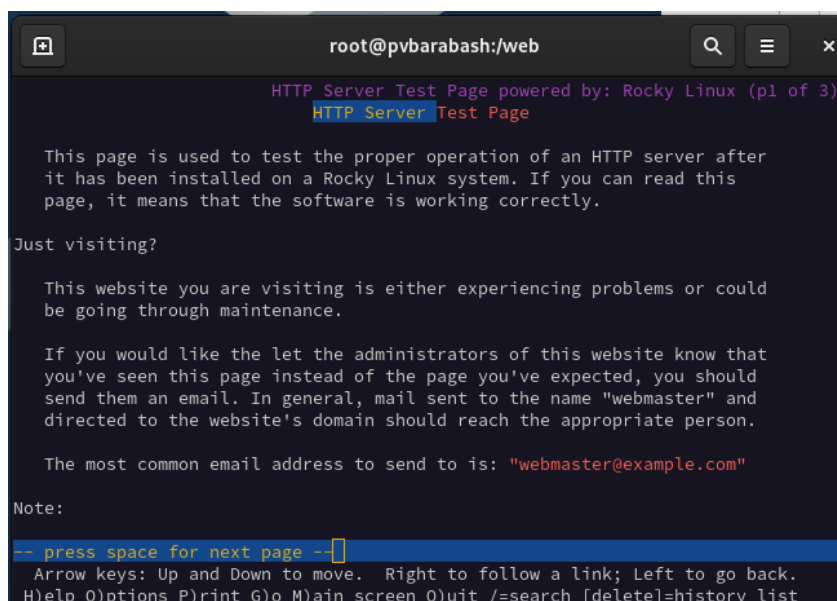


```
root@pvbarabash:/web
[root@pvbarabash web]# systemctl start httpd
[root@pvbarabash web]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@pvbarabash web]#
```

Рис. 2.23: Запуск веб-сервера и службы httpd

Задание 23. Запустите веб-сервер в текстовом браузере lynx.

Я запустила веб-сервер в текстовом браузере lynx с помощью команды lynx http://localhost (рис. 2.24).



```
root@pvbarabash:/web
HTTP Server Test Page powered by: Rocky Linux (p1 of 3)
HTTP Server 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"

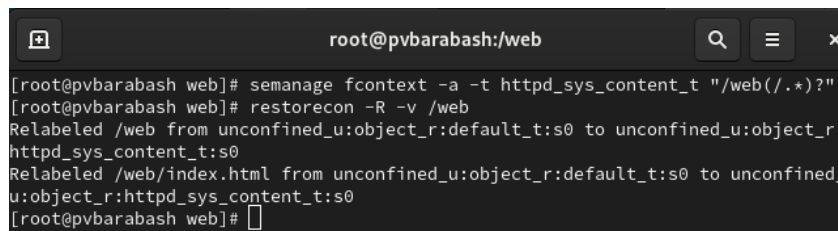
Note:
-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Рис. 2.24: Запуск веб-сервера в текстовом браузере

Я увидела веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.

Задание 24. В терминале с полномочиями администратора примените новую метку контекста к /web: semanage fcontext -a -t httpd_sys_content_t "/web(/.*)"?. Восстановите контекст безопасности.

Я использовала приведенную команду, затем я использовала команду restorecon -R -v /web, чтобы восстановить контекст безопасности (рис. 2.25).

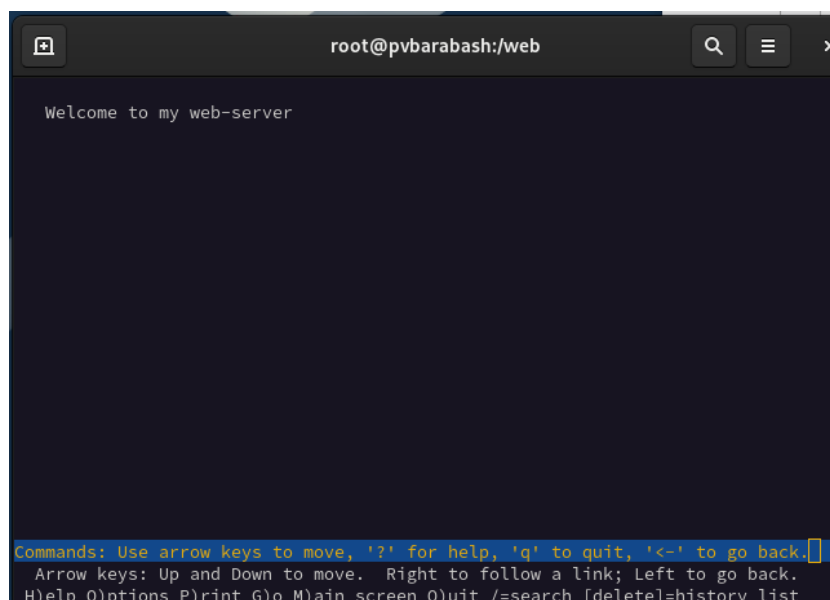


```
root@pvbarabash:/web
[root@pvbarabash web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@pvbarabash web]# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0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

Рис. 2.25: Применение новой метки контекста к /web и восстановление контекста безопасности

Задание 25. Снова обратитесь к веб-серверу.

Я использовала команду `lynx http://localhost`, чтобы вновь открыть страницу в текстовом браузере (рис. 2.26).



```
root@pvbarabash:/web
Welcome to my web-server

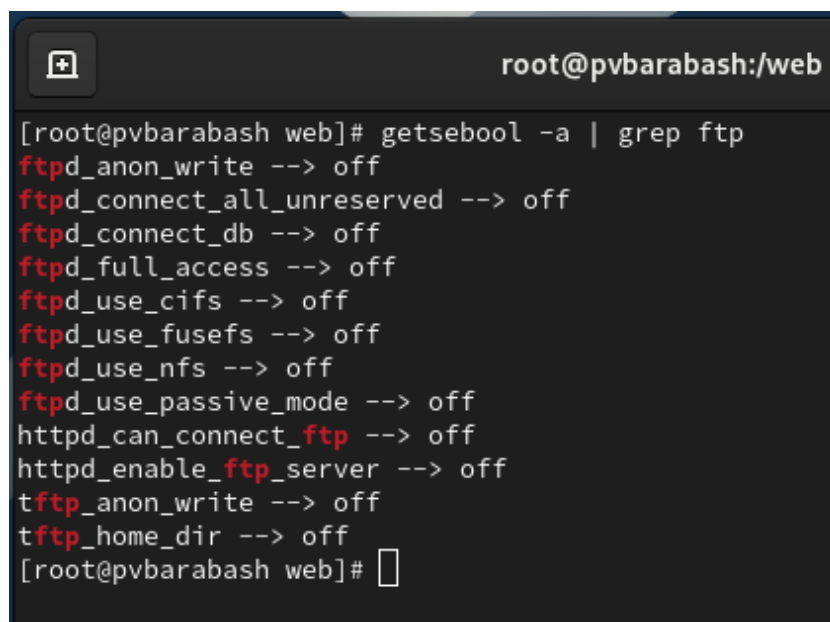
Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Рис. 2.26: Повторное открытие веб-сервера в текстовом браузере

Теперь действительно появилась запись из нашего файла `index.html`.

Задание 26. Посмотрите список переключателей SELinux для службы `ftp`.

Я использовала команду `getsebool -a | grep ftp`, чтобы посмотреть список переключателей SELinux для службы `ftp` (рис. 2.27).

A terminal window with a dark background. The title bar shows a window icon, a plus icon, and the text 'root@pvbarabash:/web'. The terminal content shows the command '[root@pvbarabash web]# getsebool -a | grep ftpd' followed by a list of SELinux booleans for the ftpd service, all set to 'off'. The booleans listed are: ftpd_anon_write, ftpd_connect_all_unreserved, ftpd_connect_db, ftpd_full_access, ftpd_use_cifs, ftpd_use_fusefs, ftpd_use_nfs, ftpd_use_passive_mode, httpd_can_connect_ftp, httpd_enable_ftp_server, tftp_anon_write, and tftp_home_dir. The prompt returns to '[root@pvbarabash web]# ' after the list.

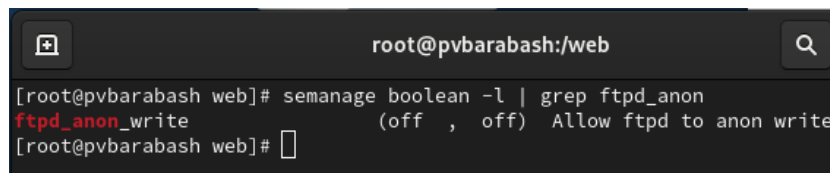
```
root@pvbarabash:/web
[root@pvbarabash web]# getsebool -a | grep ftpd
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@pvbarabash web]#
```

Рис. 2.27: Просмотр списка переключателей SELinux для службы ftp

Я увидела переключатель ftpd_anon_write с текущим значением off.

Задание 27. Для службы ftpd_anon посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен.

Я ввела команду `semanage boolean -l | grep ftpd_anon`, чтобы посмотреть список переключателей с пояснением (рис. 2.28).

A terminal window with a dark background. The title bar shows a window icon, a plus icon, the text 'root@pvbarabash:/web', and a search icon. The terminal content shows the command '[root@pvbarabash web]# semanage boolean -l | grep ftpd_anon' followed by the output for the ftpd_anon_write boolean, showing its current and default states as 'off' and an explanation: 'Allow ftpd to anon write'. The prompt returns to '[root@pvbarabash web]# ' after the output.

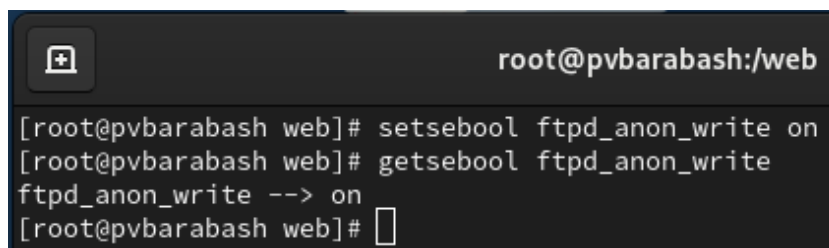
```
root@pvbarabash:/web
[root@pvbarabash web]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@pvbarabash web]#
```

Рис. 2.28: Просмотр списка переключателей с пояснением

Задание 28. Измените текущее значение переключателя для службы ftpd_anon_write с off на on. Повторно посмотрите список переключателей SELinux для службы ftpd_anon_write.

Я использовала команду `setsebool ftpd_anon_write on`, чтобы изменить текущее значение переключателя для службы ftpd_anon_write с off на on. Затем я проверила командой `getsebool ftpd_anon_write`, что действительно текущее состояние

переключателя изменилось (рис. 2.29).

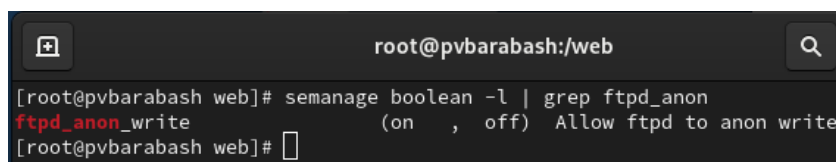


```
root@pvbarabash:/web
[root@pvbarabash web]# setsebool ftpd_anon_write on
[root@pvbarabash web]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@pvbarabash web]#
```

Рис. 2.29: Изменение переключателя для службы и проверка изменения

Задание 29. Посмотрите список переключателей с пояснением.

Я вновь посмотрела список переключателей с пояснением (рис. 2.30).



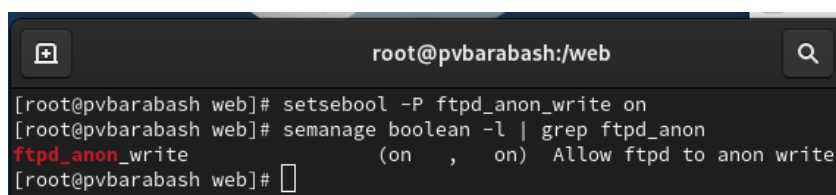
```
root@pvbarabash:/web
[root@pvbarabash web]# semmanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
[root@pvbarabash web]#
```

Рис. 2.30: Просмотр списка переключателей с пояснением

Я обратила внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Задание 30. Измените постоянное значение переключателя для службы ftpd_anon_write с off на on. Посмотрите список переключателей.

Я ввела команду `setsebool -P ftpd_anon_write on`, чтобы изменить постоянное значение переключателя службы ftpd_anon_write с off на on. А затем посмотрела список переключателей (рис. 2.31).



```
root@pvbarabash:/web
[root@pvbarabash web]# setsebool -P ftpd_anon_write on
[root@pvbarabash web]# semmanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
[root@pvbarabash web]#
```

Рис. 2.31: Изменение постоянного значения переключателя для службы и просмотр списка переключателей

Теперь и текущее значение переключателя, и постоянное включено.

3 Ответы на контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете? Команду `setenforce 0`.
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете? Команду `getsebool -a`.
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Пакет называется `polycoreutils`.
4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`? `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Файл конфигурации находится по пути: `/etc/selinux/config`. Нужно изменить параметр `SELINUX=` на `disabled`.
6. Где SELinux регистрирует все свои сообщения? SELinux регистрирует свои сообщения в журнале `/var/log/audit/audit.log` и в системном журнале (`/var/log/messages` или `/var/log/syslog` в зависимости от дистрибутива).
7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию? `seinfo -type=ftp` или `sesearch -allow -s ftp_t -t`
8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать? Ввести команду `ausearch -m avc -ts recent`. Эта команда покажет последние

сообщения AVC (Access Vector Cache), которые могут указать, блокирует ли SELinux доступ сервису.

4 Выводы

Я получила навыки работы с контекстом безопасности и политиками SELinux.