

Отчёт по лабораторной работе №9

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

1	Цель работы	6
2	Задание	7
3	Выполнение лабораторной работы	8
3.1	Управление режимами SELinux	8
3.2	Использование restorecon для восстановления контекста безопасности	14
3.3	Настройка контекста безопасности для нестандартного расположения файлов веб-сервера	17
3.4	Работа с переключателями SELinux	22
4	Контрольные вопросы + ответы	25
5	Выводы	29
6	Список литературы	30

Список иллюстраций

3.1	Режим суперпользователя	8
3.2	Состояние SELinux (1)	8
3.3	Режим работы SELinux (1)	10
3.4	Изменение режима работы SELinux на Permissive	10
3.5	Режим работы SELinux (2)	11
3.6	Открытие файла /etc/sysconfig/selinux (1)	11
3.7	Файл /etc/sysconfig/selinux (1)	11
3.8	SELINUX=disabled	11
3.9	Перезапуск системы	12
3.10	Режим работы SELinux (3)	12
3.11	Попытка изменения режима работы SELinux	12
3.12	Открытие файла /etc/sysconfig/selinux (2)	12
3.13	Файл /etc/sysconfig/selinux (2)	13
3.14	SELINUX=enforcing	13
3.15	Перезагрузка системы + предупреждающее сообщение	13
3.16	Состояние SELinux (2)	14
3.17	Контекст безопасности файла /etc/hosts (1)	14
3.18	Копирование файла /etc/hosts в домашний каталог	14
3.19	Контекст безопасности файла ~/hosts	15
3.20	Перезапись существующего файла hosts из домашнего каталога в каталог /etc	15
3.21	Контекст безопасности файла /etc/hosts (2)	15
3.22	Исправление контекста безопасности	15
3.23	Контекст безопасности файла /etc/hosts (3)	16
3.24	Массовое исправление контекста безопасности	16
3.25	Перезагрузка системы + загрузочные сообщения	16
3.26	Установка httpd	17
3.27	Установка lynx	17
3.28	Создание хранилища для файлов web-сервера	17
3.29	Создание файла index.html в каталоге с контентом веб-сервера	18
3.30	Открытие файла index.html	18
3.31	Файл index.html	18
3.32	Редактирование файла index.html	18
3.33	Открытие файла etc/httpd/conf/httpd.conf	18
3.34	Файл etc/httpd/conf/httpd.conf	19
3.35	Редактирование файла etc/httpd/conf/httpd.conf (1)	19
3.36	Редактирование файла etc/httpd/conf/httpd.conf (2)	20

3.37	Запуск веб-сервера и службы httpd	20
3.38	lynx http://localhost (1)	20
3.39	Веб-страница Red Hat по умолчанию	21
3.40	Применение новой метки контекста к /web	21
3.41	Восстановление контекста безопасности	21
3.42	lynx http://localhost (2)	22
3.43	Наша пользовательская веб-страница	22
3.44	Список переключателей SELinux для службы ftp	23
3.45	Список переключателей с пояснением для службы ftpd_anon . . .	23
3.46	Изменение текущего значения переключателя службы ftpd_anon_write с off на on	23
3.47	Список переключателей SELinux для службы ftpd_anon_write . . .	23
3.48	Список переключателей с пояснением для службы ftpd_anon_write (1)	24
3.49	Изменение постоянного значения переключателя для службы ftpd_anon_write с off на on	24
3.50	Список переключателей с пояснением для службы ftpd_anon_write (2)	24
4.1	Вопрос №1	25
4.2	Вопрос №2	25
4.3	Вопрос №4 (1)	26
4.4	Вопрос №4 (2)	26
4.5	Вопрос №5 (1)	26
4.6	Вопрос №5 (2)	27
4.7	Вопрос №6	27
4.8	Вопрос №7	28

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Задание

1. Продемонстрировать навыки по управлению режимами SELinux.
2. Продемонстрировать навыки по восстановлению контекста безопасности SELinux.
3. Настроить контекст безопасности для нестандартного расположения файлов вебслужбы.
4. Продемонстрировать навыки работы с переключателями SELinux.

3 Выполнение лабораторной работы

3.1 Управление режимами SELinux

Запускаем терминала и получаем полномочия суперпользователя, используя *su* - (рис. 3.1)

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

Рис. 3.1: Режим суперпользователя

Посмотрим текущую информацию о состоянии SELinux, используя *sestatus -v* (рис. 3.2)

```
[root@eavernikovskaya ~]# 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  
[root@eavernikovskaya ~]#
```

Рис. 3.2: Состояние SELinux (1)

Основная информация о статусе SELinux:

- **SELinux status:** enabled — SELinux включен в системе
- **SELinuxfs mount:** /sys/fs/selinux — путь, где монтируется файловая система SELinux
- **SELinux root directory:** /etc/selinux — корневой каталог, в котором хранятся конфигурационные файлы SELinux
- **Loaded policy name:** targeted — в системе загружена политика targeted, которая защищает определенные сервисы
- **Current mode:** enforcing — SELinux работает в режиме enforcing, то есть все запрещенные действия блокируются
- **Mode from config file:** enforcing — конфигурационный файл настроен на режим enforcing
- **Policy MLS status:** enabled — включена поддержка многоуровневой безопасности (MLS)
- **Policy deny_unknown status:** allowed — неизвестные действия разрешены, но это обычно не рекомендуется
- **Memory protection checking:** actual (secure) — используется актуальная защита памяти
- **Max kernel policy version:** 33 — максимальная версия политики, поддерживаемая ядром

Контексты процессов:

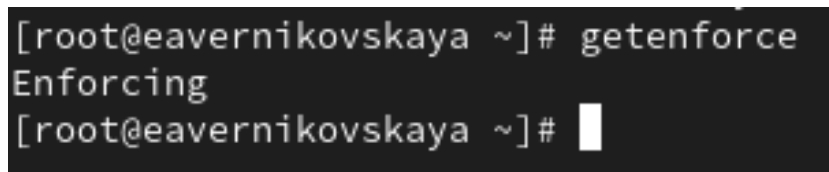
- **Current context:** unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 — текущий контекст пользователя, использующего терминал, показывает, что пользователь не ограничен политиками SELinux
- **Init context:** system_u:system_r:init_t:s0 — контекст процесса инициализации (init), который запускается от имени system_u
- **/usr/sbin/sshd:** system_u:system_r:sshd_t:s0-s0:c0.c1023 — контекст для демона sshd (Secure Shell Daemon), запущенного от имени system_u, чтобы ограничить его права в системе

Контексты файлов:

Каждая строка в этом разделе показывает файлы и процессы с их соответствующими SELinux-контекстами

- **Controlling terminal:** `unconfined_u:object_r:user_devpts_t:s0` — терминал, к которому подключен пользователь, в контексте `user_devpts_t`
- **/etc/passwd и /etc/shadow:** находятся в контексте `passwd_file_t` и `shadow_t`, что ограничивает доступ к этим файлам для повышения безопасности
- **/bin/bash:** контекст `shell_exec_t`, указывающий, что это исполняемый файл командной оболочки
- **/usr/sbin/sshd:** контекст `sshd_exec_t`, что позволяет SELinux определять, что этот файл — исполняемый файл SSH

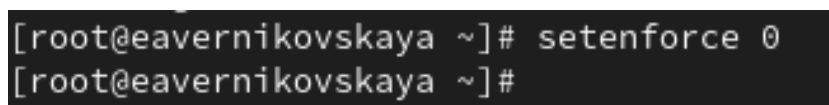
Посмотрим, в каком режиме работает SELinux: *getenforce*. По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing) (рис. 3.3)



```
[root@eavernikovskaya ~]# getenforce
Enforcing
[root@eavernikovskaya ~]#
```

Рис. 3.3: Режим работы SELinux (1)

Изменим режим работы SELinux на разрешающий (Permissive): *setenforce 0* (рис. 3.4)



```
[root@eavernikovskaya ~]# setenforce 0
[root@eavernikovskaya ~]#
```

Рис. 3.4: Изменение режима работы SELinux на Permissive

После, снова вводим *getenforce* (рис. 3.5)

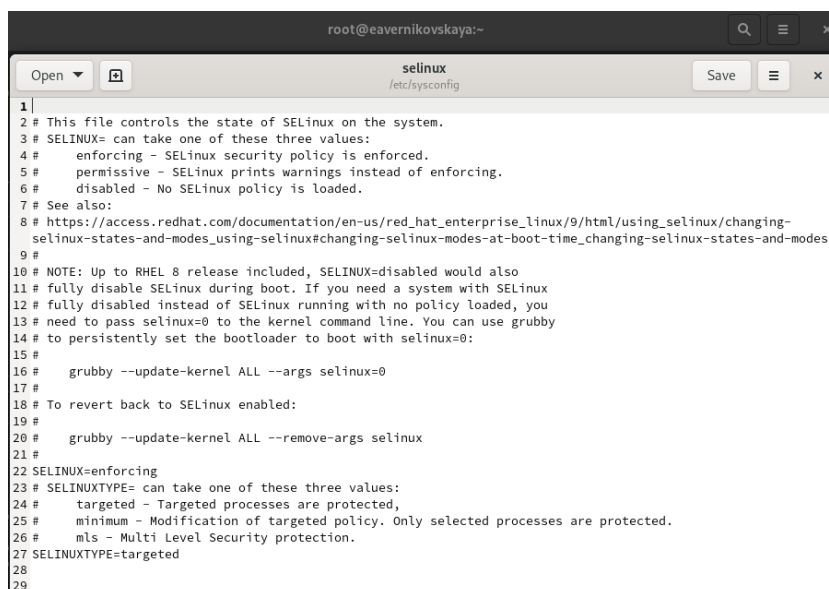
```
[root@eavernikovskaya ~]# getenforce
Permissive
[root@eavernikovskaya ~]#
```

Рис. 3.5: Режим работы SELinux (2)

В файле `/etc/sysconfig/selinux` с помощью редактора устанавливаем параметр `disabled: SELINUX=disabled` (рис. 3.6), (рис. 3.7), (рис. 3.8)

```
[root@eavernikovskaya ~]# gedit /etc/sysconfig/selinux
```

Рис. 3.6: Открытие файла `/etc/sysconfig/selinux` (1)



```
1 |
2 # This file controls the state of SELinux on the system.
3 # SELINUX= can take one of these three values:
4 #   enforcing - SELinux security policy is enforced.
5 #   permissive - SELinux prints warnings instead of enforcing.
6 #   disabled - No SELinux policy is loaded.
7 # See also:
8 # https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-
9 # selinux-states-and-modes_using-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
10 # NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
11 # fully disable SELinux during boot. If you need a system with SELinux
12 # fully disabled instead of SELinux running with no policy loaded, you
13 # need to pass selinux=0 to the kernel command line. You can use grubby
14 # to persistently set the bootloader to boot with selinux=0:
15 #
16 #   grubby --update-kernel ALL --args selinux=0
17 #
18 # To revert back to SELinux enabled:
19 #
20 #   grubby --update-kernel ALL --remove-args selinux
21 #
22 SELINUX=enforcing
23 # SELINUXTYPE= can take one of these three values:
24 #   targeted - Targeted processes are protected,
25 #   minimum - Modification of targeted policy. Only selected processes are protected.
26 #   mls - Multi Level Security protection.
27 SELINUXTYPE=targeted
28
29
```

Рис. 3.7: Файл `/etc/sysconfig/selinux` (1)

```
21 #
22 SELINUX=disabled
```

Рис. 3.8: `SELINUX=disabled`

Далее перезапускаем систему (рис. 3.9)

```
[root@eavernikovskaya ~]# reboot
```

Рис. 3.9: Перезапуск системы

После перезагрузки запускаем терминал и получаем полномочия администратора. Далее смотрим статус SELinux. Мы увидим, что SELinux теперь отключён (рис. 3.10)

```
[root@eavernikovskaya ~]# getenforce  
Disabled  
[root@eavernikovskaya ~]#
```

Рис. 3.10: Режим работы SELinux (3)

Попробуем переключить режим работы SELinux: *setenforce 1*. Мы не сможем этого сделать, так как SELinux отключён (рис. 3.11)

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

Рис. 3.11: Попытка изменения режима работы SELinux

В файле `/etc/sysconfig/selinux` с помощью редактора устанавливаем параметр `enforcing`: *SELINUX=enforcing* (рис. 3.12), (рис. 3.13), (рис. 3.14)

```
[root@eavernikovskaya ~]# gedit /etc/sysconfig/selinux
```

Рис. 3.12: Открытие файла `/etc/sysconfig/selinux` (2)

```
root@eavernikovskaya:~  
selinux  
/etc/sysconfig  
1  
2 # This file controls the state of SELinux on the system.  
3 # SELinux= can take one of these three values:  
4 #     enforcing - SELinux security policy is enforced.  
5 #     permissive - SELinux prints warnings instead of enforcing.  
6 #     disabled - No SELinux policy is loaded.  
7 # See also:  
8 # https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-  
selinux-states-and-modes_using_selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes  
9 #  
10 # NOTE: Up to RHEL 8 release included, SELinux=disabled would also  
11 # fully disable SELinux during boot. If you need a system with SELinux  
12 # fully disabled instead of SELinux running with no policy loaded, you  
13 # need to pass selinux=0 to the kernel command line. You can use grubby  
14 # to persistently set the bootloader to boot with selinux=0:  
15 #  
16 #     grubby --update-kernel ALL --args selinux=0  
17 #  
18 # To revert back to SELinux enabled:  
19 #  
20 #     grubby --update-kernel ALL --remove-args selinux  
21 #  
22 SELINUX=disabled  
23 # SELINUXTYPE= can take one of these three values:  
24 #     targeted - Targeted processes are protected,  
25 #     minimum - Modification of targeted policy. Only selected processes are protected.  
26 #     mls - Multi Level Security protection.  
27 SELINUXTYPE=targeted  
28  
29
```

Рис. 3.13: Файл /etc/sysconfig/selinux (2)

```
21 #  
22 SELINUX=enforcing
```

Рис. 3.14: SELINUX=enforcing

Снова перезагружаем систему. Во время загрузки системы мы, получили предупреждающее сообщение о необходимости восстановления меток SELinux (рис. 3.15)

```
[ 0.060978] RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to  
RETbleed attacks, data leaks possible!  
[ 1.394049] systemd[1]: Invalid DMI field header.  
[ 2.223446] Warning: Unmaintained driver is detected: e1000  
[ 2.508165] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on  
an unsupported hypervisor.  
[ 2.508166] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b  
roken.  
[ 2.508167] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g  
raphics device to avoid problems.  
[ 6.611082] selinux-autorelabel[700]: *** Warning -- SELinux targeted policy relabel is required.  
[ 6.612081] selinux-autorelabel[700]: *** Relabeling could take a very long time, depending on file  
[ 6.612328] selinux-autorelabel[700]: *** system size and speed of hard drives.  
[ 6.623363] selinux-autorelabel[700]: Running: /sbin/fixfiles -T 0 restore  
[ 20.214337] selinux-autorelabel[706]: Warning: Skipping the following R/O filesystems:  
[ 20.214720] selinux-autorelabel[706]: /run/credentials/systemd-sysctl.service  
[ 20.214823] selinux-autorelabel[706]: /run/credentials/systemd-tmpfiles-setup-dev.service  
[ 20.215000] selinux-autorelabel[706]: /run/credentials/systemd-tmpfiles-setup.service  
[ 20.216047] selinux-autorelabel[706]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /sys  
/debug /sys/kernel/tracing
```

Рис. 3.15: Перезагрузка системы + предупреждающее сообщение

После перезагрузки в терминале с полномочиями администратора посмотрим

текущую информацию о состоянии SELinux. Система работает в принудительном режиме (enforcing) использования SELinux (рис. 3.16)

```
[root@eavernikovskaya ~]# 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
[root@eavernikovskaya ~]#
```

Рис. 3.16: Состояние SELinux (2)

3.2 Использование restorecon для восстановления контекста безопасности

Посмотрим контекст безопасности файла `/etc/hosts`: `ls -Z /etc/hosts`. Мы увидим, что у файла есть метка контекста `net_conf_t` (рис. 3.17)

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

Рис. 3.17: Контекст безопасности файла `/etc/hosts` (1)

Скопируем файл `/etc/hosts` в домашний каталог, с помощью `cp /etc/hosts ~/` (рис. 3.18)

```
[root@eavernikovskaya ~]# cp /etc/hosts ~/
[root@eavernikovskaya ~]#
```

Рис. 3.18: Копирование файла `/etc/hosts` в домашний каталог

Проверяем контекст файла `~/hosts`: `ls -Z ~/hosts`. Поскольку копирование считается созданием нового файла, то параметр контекста в файле `~/hosts`, расположенном в домашнем каталоге, станет `admin_home_t` (рис. 3.19)

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

Рис. 3.19: Контекст безопасности файла `~/hosts`

Попытаемся перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`: `mv ~/hosts /etc` (рис. 3.20)

```
[root@eavernikovskaya ~]# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? y
[root@eavernikovskaya ~]#
```

Рис. 3.20: Перезапись существующего файла `hosts` из домашнего каталога в каталог `/etc`

Далее проверим, что тип контекста по-прежнему установлен на `admin_home_t`: `ls -Z /etc/hosts` (рис. 3.21)

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

Рис. 3.21: Контекст безопасности файла `/etc/hosts` (2)

Далее исправим контекст безопасности: `restorecon -v /etc/hosts`. Опция `-v` покажет процесс изменения (рис. 3.22)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.22: Исправление контекста безопасности

Проверим, что тип контекста изменился (рис. 3.23)

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

Рис. 3.23: Контекст безопасности файла /etc/hosts (3)

Для массового исправления контекста безопасности на файловой системе вводим `touch /.autorelabel` (рис. 3.24)

```
[root@eavernikovskaya ~]# touch /.autorelabel
[root@eavernikovskaya ~]#
```

Рис. 3.24: Массовое исправление контекста безопасности

После перезапускаем систему. Во время перезапуска нажимаем клавишу Esc, чтобы мы видели загрузочные сообщения. Мы увидим, что файловая система автоматически перемаркирована (рис. 3.25)

```
[ OK ] Finished Remount Root and Kernel File Systems.
[ OK ] Reached target Preparation for Network.
[ OK ] Reached target Swaps.
      Mounting FUSE Control File System...
      Mounting Kernel Configuration File System...
      Starting Load/Save OS Random Seed...
      Starting Apply Kernel Variables...
      Starting Create Static Device Nodes in /dev...
[ OK ] Started Journal Service.
[ OK ] Finished Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling.
[ OK ] Mounted FUSE Control File System.
[ OK ] Mounted Kernel Configuration File System.
      Starting Flush Journal to Persistent Storage...
[ OK ] Finished Load/Save OS Random Seed.
[ OK ] Finished Apply Kernel Variables.
[ OK ] Finished Coldplug All udev Devices.
      Starting Wait for udev To Complete Device Initialization...
[ OK ] Finished Create Static Device Nodes in /dev.
      Starting Rule-based Manager for Device Events and Files...
[ OK ] Finished Flush Journal to Persistent Storage.
[ OK ] Started Rule-based Manager for Device Events and Files.
      Starting Load Kernel Module configs...
[ OK ] Finished Load Kernel Module configs.
      Starting Load Kernel Module fuse...
[ OK ] Finished Load Kernel Module fuse.
[ OK ] Started /usr/sbin/lockd --autoactivation event rd.
[ OK ] Finished Wait for udev To Complete Device Initialization.
[ OK ] Reached target Preparation for Local File Systems.
      Mounting /boot...
[ OK ] Mounted /boot.
[ OK ] Reached target Local File Systems.
      Starting Tell Plymouth To Write Out Runtime Data...
      Starting Automatic Boot Loader Update...
      Starting Create Volatile Files and Directories...
[ OK ] Finished Automatic Boot Loader Update.
[ OK ] Finished Tell Plymouth To Write Out Runtime Data.
[ OK ] Finished Create Volatile Files and Directories.
      Starting Record System Boot/Shutdown in UTMP...
[ OK ] Finished Record System Boot/Shutdown in UTMP.
[ OK ] Reached target System Initialization.
[ OK ] Started Manage Sound Card State (restore and store).
[ OK ] Reached target Sound Card.
      Starting Restore /run/intrinsics on shutdown...
      Starting Relabel all filesystems...
[ OK ] Started Restore /run/intrinsics on shutdown.
7.199289] selinux-autorelabel[781]: *** Warning -- SELinux targeted policy relabel is required.
7.288629] selinux-autorelabel[781]: *** Relabeling could take a very long time, depending on file
7.281873] selinux-autorelabel[781]: *** system size and speed of hard drives.
7.213832] selinux-autorelabel[781]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 3.25: Перезагрузка системы + загрузочные сообщения

3.3 Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

Устанавливаем необходимое программное обеспечение (рис. 3.26), (рис. 3.27)

```
[root@eavernikovskaya ~]# dnf -y install httpd
Rocky Linux 9 - BaseOS                               3.0 kB/s | 4.1 kB  00:01
Rocky Linux 9 - BaseOS                               1.9 MB/s | 2.3 MB  00:01
Rocky Linux 9 - AppStream                             10 kB/s | 4.5 kB  00:00
Rocky Linux 9 - AppStream                             3.5 MB/s | 8.0 MB  00:02
Rocky Linux 9 - Extras                                5.8 kB/s | 2.9 kB  00:00
Package httpd-2.4.57-11.el9_4.1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@eavernikovskaya ~]#
```

Рис. 3.26: Установка httpd

```
[root@eavernikovskaya ~]# dnf -y install lynx
Last metadata expiration check: 0:00:25 ago on Fri 01 Nov 2024 01:27:52 PM MSK.
Dependencies resolved.
=====
Package                Architecture      Version           Repository         Size
=====
Installing:
lynx                   x86_64            2.8.9-20.el9      appstream           1.5 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 1.5 M
Installed size: 6.1 M
Downloading Packages:
lynx-2.8.9-20.el9.x86_64.rpm                                1.3 MB/s | 1.5 MB  00:01
-----
Total                                                    816 kB/s | 1.5 MB  00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : lynx-2.8.9-20.el9.x86_64                    1/1
  Installing     : lynx-2.8.9-20.el9.x86_64                    1/1
  Running scriptlet: lynx-2.8.9-20.el9.x86_64                    1/1
  Verifying      : lynx-2.8.9-20.el9.x86_64                    1/1

Installed:
  lynx-2.8.9-20.el9.x86_64

Complete!
[root@eavernikovskaya ~]#
```

Рис. 3.27: Установка lynx

Создаём новое хранилище для файлов web-сервера: `mkdir /web` (рис. 3.28)

```
[root@eavernikovskaya ~]# mkdir /web
[root@eavernikovskaya ~]#
```

Рис. 3.28: Создание хранилища для файлов web-сервера

Создаём файл `index.html` в каталоге с контентом веб-сервера (рис. 3.29)

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

Рис. 3.29: Создание файла index.html в каталоге с контентом веб-сервера

Пишем в созданном файле index.html следующий текст: Welcome to my web-server (рис. 3.30), (рис. 3.31), (рис. 3.32)

```
[root@eavernikovskaya web]# gedit /web/index.html
```

Рис. 3.30: Открытие файла index.html

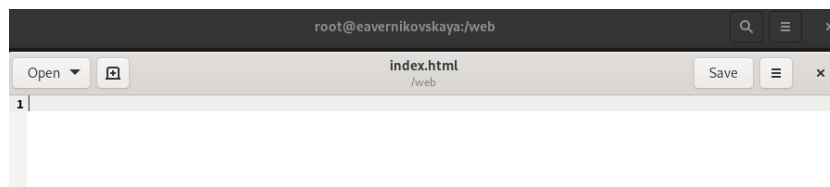


Рис. 3.31: Файл index.html

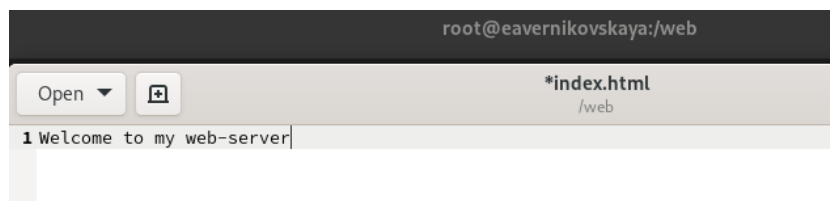


Рис. 3.32: Редактирование файла index.html

В файле /etc/httpd/conf/httpd.conf закомментируем строку *DocumentRoot* “/var/www/html” и ниже добавим строку *DocumentRoot* “/web” (рис. 3.33), (рис. 3.34), (рис. 3.35)

```
[root@eavernikovskaya web]# gedit /etc/httpd/conf/httpd.conf
```

Рис. 3.33: Открытие файла etc/httpd/conf/httpd.conf

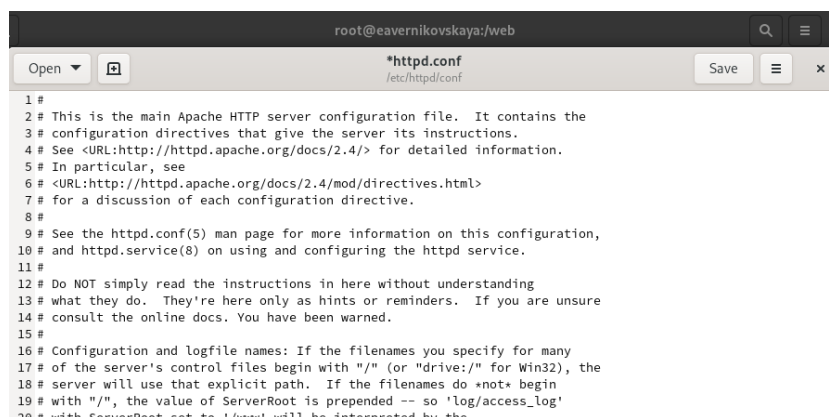


Рис. 3.34: Файл etc/httpd/conf/httpd.conf

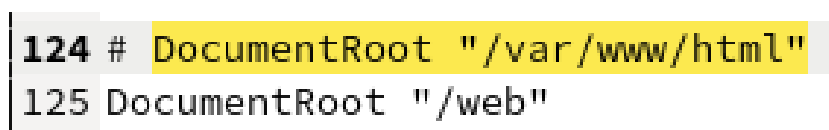


Рис. 3.35: Редактирование файла etc/httpd/conf/httpd.conf (1)

Затем в этом же файле ниже прокомментируем раздел

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

и добавим следующий раздел, определяющий правила доступа: (рис. 3.36)

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

```
# <Directory "/var/www">
    # AllowOverride None
    # Allow open access:
    # Require all granted
# </Directory>

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

Рис. 3.36: Редактирование файла etc/httpd/conf/httpd.conf (2)

Запускаем веб-сервер и службу httpd (рис. 3.37)

```
[root@eavernikovskaya web]# systemctl start httpd
[root@eavernikovskaya web]# systemctl enable httpd
[root@eavernikovskaya web]#
```

Рис. 3.37: Запуск веб-сервера и службы httpd

В терминале под учётной записью нашего пользователя обращаемся к веб-серверу в текстовом браузере lynx: `lynx http://localhost` (рис. 3.38)

```
[eavernikovskaya@eavernikovskaya ~]$ lynx http://localhost
```

Рис. 3.38: lynx http://localhost (1)

После этого мы увидим веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html (для выхода из lynx нажимается q) (рис. 3.39)

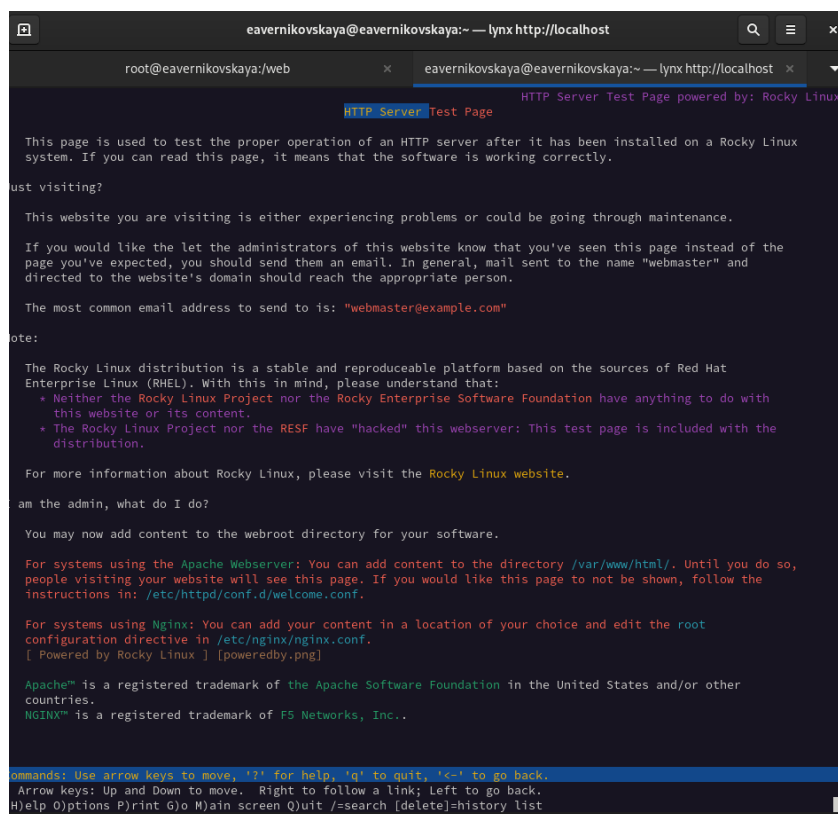


Рис. 3.39: Веб-страница Red Hat по умолчанию

В терминале с полномочиями администратора применяем новую метку контекста к `/web`: `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"` (рис. 3.40)

```
[root@eavernikovskaya web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@eavernikovskaya web]#
```

Рис. 3.40: Применение новой метки контекста к `/web`

Восстановим контекст безопасности: `restorecon -R -v /web` (рис. 3.41)

```
[root@eavernikovskaya 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@eavernikovskaya web]#
```

Рис. 3.41: Восстановление контекста безопасности

В терминале под учётной записью нашего пользователя снова обращаемся к веб-серверу: `lynx http://localhost`. Теперь мы получили доступ к своей пользовательской веб-странице. На экране есть запись «Welcome to my web-server» (рис. 3.42), (рис. 3.43)

```
[eavernikovskaya@eavernikovskaya ~]$ lynx http://localhost
```

Рис. 3.42: lynx http://localhost (2)

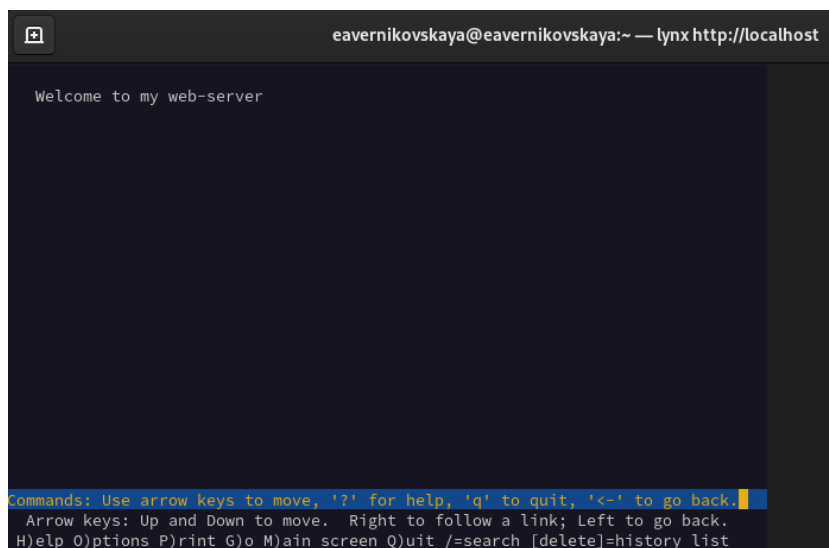


Рис. 3.43: Наша пользовательская веб-страница

3.4 Работа с переключателями SELinux

Посмотрим список переключателей SELinux для службы ftp: `getsebool -a | grep ftp`. Мы увидим переключатель `ftpd_anon_write` с текущим значением `off` (рис. 3.44)

```
[root@eavernikovskaya ~]# getsebool -a | grep ftp
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@eavernikovskaya ~]#
```

Рис. 3.44: Список переключателей SELinux для службы ftp

Для службы `ftpd_anon` посмотрим список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен: `semanage boolean -l | grep ftpd anon` (рис. 3.45)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (off , off) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 3.45: Список переключателей с пояснением для службы ftpd_anon

Изменим текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`: `setsebool ftpd_anon_write on` (рис. 3.46)

```
[root@eavernikovskaya ~]# setsebool ftpd_anon_write on
[root@eavernikovskaya ~]#
```

Рис. 3.46: Изменение текущего значения переключателя службы ftpd_anon_write с off на on

Повторно смотрим список переключателей SELinux для службы `ftpd_anon_write`: `getsebool ftpd_anon_write` (рис. 3.47)

```
[root@eavernikovskaya ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@eavernikovskaya ~]#
```

Рис. 3.47: Список переключателей SELinux для службы ftpd_anon_write

Посмотрим список переключателей с пояснением: *semanage boolean -l | grep ftpd_anon*. Мы видим, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена (рис. 3.48)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , off) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 3.48: Список переключателей с пояснением для службы ftpd_anon_write (1)

Изменим постоянное значение переключателя для службы ftpd_anon_write с off на on: *setsebool -P ftpd_anon_write on* (рис. 3.49)

```
[root@eavernikovskaya ~]# setsebool -P ftpd_anon_write on
[root@eavernikovskaya ~]#
```

Рис. 3.49: Изменение постоянного значения переключателя для службы ftpd_anon_write с off на on

Снова посмотрим список переключателей: *semanage boolean -l | grep ftpd_anon*. Теперь постоянная настройка включена (рис. 3.50)

```
[root@eavernikovskaya ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (on , on) Allow ftpd to anon write
[root@eavernikovskaya ~]#
```

Рис. 3.50: Список переключателей с пояснением для службы ftpd_anon_write (2)

4 Контрольные вопросы + ответы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?

setenforce 0 (рис. 4.1)

```
[root@eavernikovskaya ~]# setenforce 0  
[root@eavernikovskaya ~]#
```

Рис. 4.1: Вопрос №1

2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?

getsebool -a (рис. 4.2)

```
[eavernikovskaya@eavernikovskaya ~]$ getsebool -a  
abrt_anon_write --> off  
abrt_handle_event --> off  
abrt_upload_watch_anon_write --> on  
antivirus_can_scan_system --> off  
antivirus_use_jit --> off  
auditadm_exec_content --> on
```

Рис. 4.2: Вопрос №2

3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?

audit2allow

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(/.*)?" restorecon -R -v /web` (рис. 4.3), (рис. 4.4)

```
[root@eavernikovskaya web]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
[root@eavernikovskaya web]#
```

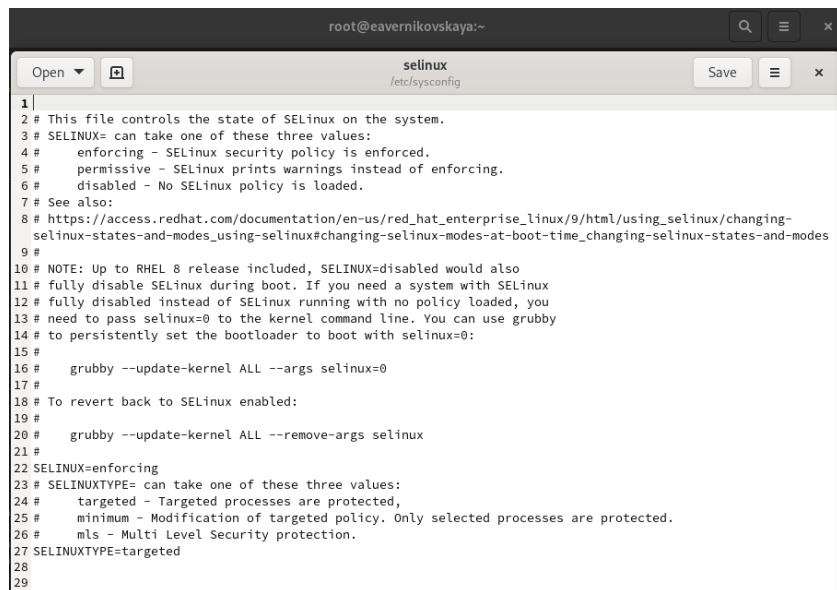
Рис. 4.3: Вопрос №4 (1)

```
[root@eavernikovskaya 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@eavernikovskaya web]#
```

Рис. 4.4: Вопрос №4 (2)

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?

`/etc/sysconfig/selinux` (рис. 4.5), (рис. 4.6)

The image shows a terminal window with a text editor open to the file `/etc/sysconfig/selinux`. The file contains configuration for SELinux, including comments about enforcing, permissive, and disabled states, and instructions on how to use `grubby` to update the kernel arguments for SELinux. The file is numbered line-by-line from 1 to 29.

```
1
2 # This file controls the state of SELinux on the system.
3 # SELINUX= can take one of these three values:
4 #   enforcing - SELinux security policy is enforced.
5 #   permissive - SELinux prints warnings instead of enforcing.
6 #   disabled - No SELinux policy is loaded.
7 # See also:
8 # https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-
9 # selinux-states-and-modes_using-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
10 #
11 # NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
12 # fully disable SELinux during boot. If you need a system with SELinux
13 # fully disabled instead of SELinux running with no policy loaded, you
14 # need to pass selinux=0 to the kernel command line. You can use grubby
15 # to persistently set the bootloader to boot with selinux=0:
16 #
17 # grubby --update-kernel ALL --args selinux=0
18 #
19 # To revert back to SELinux enabled:
20 #
21 # grubby --update-kernel ALL --remove-args selinux
22 #
23 SELINUX=enforcing
24 # SELINUXTYPE= can take one of these three values:
25 #   targeted - Targeted processes are protected,
26 #   minimum - Modification of targeted policy. Only selected processes are protected.
27 #   mls - Multi Level Security protection.
28 SELINUXTYPE=targeted
29
```

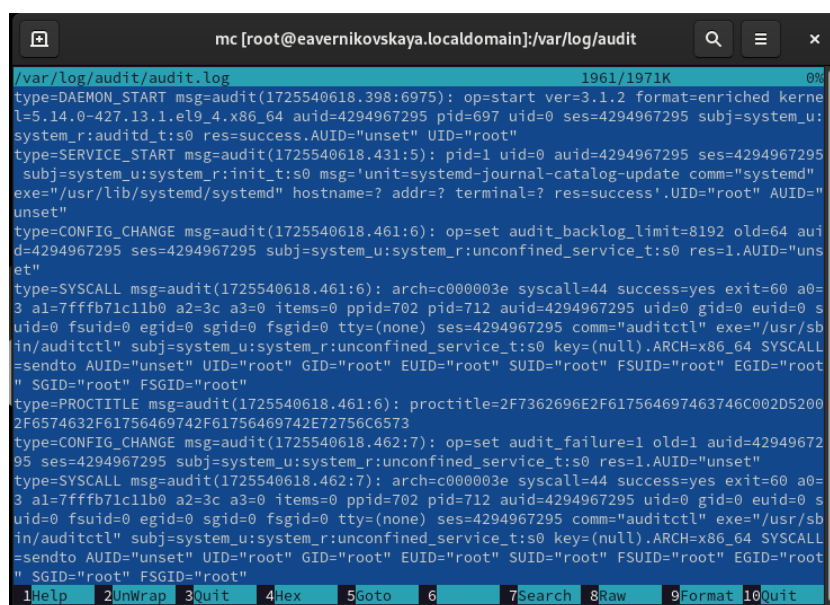
Рис. 4.5: Вопрос №5 (1)

```
21 #
22 SELINUX=disabled
```

Рис. 4.6: Вопрос №5 (2)

6. Где SELinux регистрирует все свои сообщения?

в /var/log/audit/audit.log (рис. 4.7)



```
mc [root@eavernikovskaya.localdomain]:/var/log/audit
/var/log/audit/audit.log 1961/1971K 0%
type=DAEMON_START msg=audit(1725540618.398:6975): op=start ver=3.1.2 format=enriched kernel=5.14.0-427.13.1.el9_4.x86_64 aid=4294967295 pid=697 uid=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=success.AUID="unset" UID="root"
type=SERVICE_START msg=audit(1725540618.431:5): pid=1 uid=0 aid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'.AUID="root" AUID="unset"
type=CONFIG_CHANGE msg=audit(1725540618.461:6): op=set audit_backlog_limit=8192 old=64 aid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=1.AUID="unset"
type=SYSCALL msg=audit(1725540618.461:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffffb71c11b0 a2=3c a3=0 items=0 ppid=702 pid=712 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null).ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1725540618.461:6): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1725540618.462:7): op=set audit_failure=1 old=1 aid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=1.AUID="unset"
type=SYSCALL msg=audit(1725540618.462:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffffb71c11b0 a2=3c a3=0 items=0 ppid=702 pid=712 aid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system_u:system_r:unconfined_service_t:s0 key=(null).ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

Рис. 4.7: Вопрос №6

7. Вы не знаете, какие типы контекстов доступны для службы ftp. Какая команда позволяет получить более конкретную информацию?

getsebool -a | grep ftp (рис. 4.8)

```
[root@eavernikovskaya ~]# getsebool -a | grep ftp
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@eavernikovskaya ~]#
```

Рис. 4.8: Вопрос №7

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?

Просмотреть контекст безопасности процессора `ps -eZ` или `id -Z`

5 Выводы

В ходе выполнения лабораторной работы мы получили навыки и работы с контекстом безопасности и политиками SELinux

6 Список литературы

1. Лабораторная работа №9 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/1234567/mod_resource/content/1/selinux.pdf