

Лабораторная работа №9

Отчет

Устинова Виктория Вадимовна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	14
5	Ответы на контрольные вопросы	15

Список иллюстраций

3.1	переходим в андмин. и смотрим информацию, селинукс активен и работает нормально	7
3.2	SELinux работает в режиме enforcing, мы переключили его на Permissive	7
3.3	заменяем enforcing на disabled и перезапускаем систему	8
3.4	Статус стал: disabled, не удастся перкключить на режим работы потому что она отключена	8
3.5	Снова меняем, только теперь на enforcing	8
3.6	Она активна и работает в принудительном режиме все верно . . .	9
3.7	у файла есть метка контекста net_conf_t., после копирования(что считается созданием нового файла) контекст стал admin_home_t. .	9
3.8	Поддтверждаем перезаписывание файла и тип контекста все еще admin_home_t	9
3.9	Опция -v показывает процесс изменения, тип контекста изменился на net_conf_t, вводим команду и перезапускаем машину	10
3.10	нажимаем esc во время перезапуска и видим, что система перемаркирована автоматически	10
3.11	создаем новое хранилище, переходим туда и создаем файл, через редактор nano добавляем туда строчку	10
3.12	Комментируем строчку и добавляем ниже:DocumentRoot “/web”, также ниже комментируем целый раздел и вместо него пишем другое	11
3.13	Мы открыли файл и вышли из него	11
3.14	Проделили все действия, и презагружаем машину	11
3.15	Открываем и смотрим, у нас все получилось!	12
3.16	Видим что все переключатели выключены	12
3.17	Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.	12
3.18	Теперь все включено, переключатели разрешают анонимную запись на FTP сервер через селинукс	13

Список таблиц

1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

2 Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб- службы (см. раздел 9.4.3).
4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

3 Выполнение лабораторной работы

Посмотрите текущую информацию о состоянии SELinux(рис. 3.1).

```
[root@vvustinova ~]# 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-s
```

Рис. 3.1: переходим в андмин. и смотрим информацию, селинукс активен и работает нормально

Посмотрите, в каком режиме работает SELinux, измените режим работы SELinux на разрешающий (Permissive)(рис. 3.2).

```
[root@vvustinova ~]# getenforce
Enforcing
[root@vvustinova ~]# setenforce 0
[root@vvustinova ~]# getenforce
Permissive
[root@vvustinova ~]# nano
```

Рис. 3.2: SELinux работает в режиме enforcing, мы переключили его на Permissive

В файле /etc/sysconfig/selinux с помощью редактора установите disabled(рис. 3.3).

```
GNU nano 5.6.1 /etc/sysconfig/selinux
# 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
```

Рис. 3.3: заменяем enforcing на disabled и перезапускаем систему

После перезагрузки, посмотрите статус SELinux, попробуйте переключить режим работы SELinux(рис. 3.4).

```
[vvustinova@vvustinova ~]$ su -
Пароль:
[root@vvustinova ~]# getenforce
Disabled
[root@vvustinova ~]# setenforce 1
setenforce: SELinux is disabled
[root@vvustinova ~]# nano /etc/sysconfig/selinux
```

Рис. 3.4: Статус стал: disabled, не удастся переключить на режим работы потому что она отключена

Откройте файл /etc/sysconfig/selinux с помощью редактора и установите enforcing(рис. 3.5).

```
GNU nano 5.6.1 /etc/sysconfig/selinux
# 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
```

Рис. 3.5: Снова меняем, только теперь на enforcing

После перезагрузки, убедитесь, что система работает в принудительном режиме (enforcing) использования SELinux.(рис. 3.6).

```
[vvustinova@vvustinova ~]$ su -
Пароль:
[root@vvustinova ~]# 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:
```

Рис. 3.6: Она активна и работает в принудительном режиме все верно

Посмотрите контекст безопасности файла /etc/hosts, Скопируйте файл /etc/hosts в домашний каталог, Проверьте контекст файла ~/hosts(рис. 3.7).

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

Рис. 3.7: у файла есть метка контекста net_conf_t., после копирования(что считается созданием нового файла) контекст стал admin_home_t.

Попытайтесь перезаписать существующий файл hosts из домашнего каталога в каталог /etc, убедитесь, что тип контекста по-прежнему установлен на admin_home_t(рис. 3.8).

```
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@vvustinova ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
[root@vvustinova ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
```

Рис. 3.8: Подтверждаем перезаписывание файла и тип контекста все еще admin_home_t

Исправьте контекст безопасности, убедитесь, что тип контекста изменился,

для массового исправления контекста безопасности на файловой системе введите(рис. 3.9).

```
[root@vvustinova ~]# 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@vvustinova ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@vvustinova ~]# touch /.autorelabel
[root@vvustinova ~]#
```

Рис. 3.9: Опция -v показывает процесс изменения, тип контекста изменился на net_conf_t, вводим команду и перезапускаем машину

Во время перезапуска не забудьте нажать клавишу Esc на клавиатуре, чтобы вы видели загрузочные сообщения(рис. 3.10).

```
[ OK ] Finished Automatic Boot Loader Update.
[ 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/initramfs on shutdown...
Starting Relabel all filesystems...
[ OK ] Finished Restore /run/initramfs on shutdown.
46.6792981 selinux-autorelabel[781]: *** Warning -- SELinux targeted policy relabel is required.
46.6839761 selinux-autorelabel[781]: *** Relabeling could take a very long time, depending on file
46.6858531 selinux-autorelabel[781]: *** system size and speed of hard drives.
46.7284861 selinux-autorelabel[781]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 3.10: нажимаем esc во время перезапуска и видим, что система перемаркирована автоматически

Создайте новое хранилище для файлов web-сервера, создайте файл index.html в каталоге с контентом веб-сервера, и поместите туда: Welcome to my web-server(рис. 3.11).

```
Выполнено.
[root@vvustinova ~]# mkdir /web
[root@vvustinova ~]# cd /web
[root@vvustinova web]# touch index.html
[root@vvustinova web]# nano index.html
```

Рис. 3.11: создаем новое хранилище, переходим туда и создаем файл, через редактор nano добавляем туда строку

В файле /etc/httpd/conf/httpd.conf закомментируйте строку DocumentRoot "/var/www/html" и ниже добавьте строку(рис. 3.12).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
# symbolic links and aliases may be used to point to other locations.
#
# 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>
```

Рис. 3.12: Комментируем строчку и добавляем ниже:DocumentRoot “/web”, также ниже комментируем целый раздел и вместо него пишем другое

Запустите веб-сервер и службу httpd, в терминале под учётной записью своего пользователя при обращении к веб-серверу в текстовом браузере lynx, вы увидите веб-страницу Red Hat по умолчанию, а не содержимое только что созданного файла index.html.(рис. 3.13).

```
[root@vvustinova web]# systemctl start httpd
[root@vvustinova web]# systemctl enable httpd
[root@vvustinova web]# su vvustinova
[vvustinova@vvustinova web]$ lynx http://localhost
```

Рис. 3.13: Мы открыли файл и вышли из него

В терминале с полномочиями администратора примените новую метку контекста к /web, восстановите контекст безопасности(рис. 3.14).

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

Рис. 3.14: Проделали все действия, и перезагружаем машину

Теперь вы получите доступ к своей пользовательской веб-странице.В случае успеха на экране должна быть отображена запись «Welcome to my web-server».(рис. 3.15).

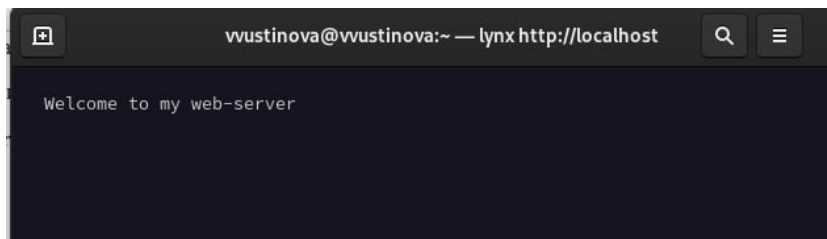


Рис. 3.15: Открываем и смотрим, у нас все получилось!

Посмотрите список переключателей SELinux для службы ftp, Вы увидите переключатель `ftpd_anon_write` с текущим значением `off`, для службы `ftpd_anon` посмотрите список переключателей (рис. 3.16).

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

Рис. 3.16: Видим что все переключатели выключены

Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`, повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`, посмотрите список переключателей с пояснением(рис. 3.17).

```
[root@vustinova ~]# setsebool ftpd_anon_write on
[root@vustinova ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@vustinova ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл.,выкл.) Allow ftpd to anon write
```

Рис. 3.17: Настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.

Измените постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`, посмотрите список переключателей:(рис. 3.18).

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

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

Рис. 3.18: Теперь все включено, переключатели разрешают анонимную запись на FTP сервер через селинукс

4 Выводы

Мы успешно получили навыки работы с контекстом безопасности и политиками SELinux.

5 Ответы на контрольные вопросы

1. Временно поставить SELinux в разрешающем режиме. Для этого используется команда `setenforce 0`. Это переводит SELinux из режима принудительного выполнения (enforcing), где он блокирует неразрешенные действия, в режим разрешения (permissive), где он лишь регистрирует нарушения, но не блокирует их. Это полезно для диагностики.
2. Список всех доступных переключателей SELinux. Чтобы получить полный список всех булевых переключателей SELinux и их текущее состояние, используйте команду `semanage boolean -l`. Эта команда также покажет краткое описание каждого переключателя.
3. Имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита? Для автоматического анализа логов SELinux и получения легко читаемых, интерпретированных сообщений об отказах (denials), а также предложений по их устранению, необходимо установить пакет `setroubleshoot-server`. Он предоставляет утилиту `sealert`.
4. Команды, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`. Для применения файлового контекста `httpd_sys_content_t` к каталогу `/web` (и всем его подкаталогам), вам потребуется выполнить две команды:
 - Сначала добавьте правило для контекста файла: `semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"`. Эта команда говорит SELinux, что данный тип контекста должен применяться к указанному пути.
 - Затем примените

это правило к файловой системе: `restorecon -Rv /web`. Эта команда изменит контексты файлов на диске в соответствии с правилами `fcontext`.

5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux? Чтобы полностью отключить SELinux, необходимо отредактировать конфигурационный файл `/etc/selinux/config`. В этом файле нужно найти строку `SELINUX=enforcing` (или `SELINUX=permissive`) и изменить ее на `SELINUX=disabled`. После сохранения файла потребуется перезагрузить систему, чтобы изменения вступили в силу.
6. Где SELinux регистрирует все свои сообщения? SELinux регистрирует все свои сообщения, включая отказы доступа (AVC denials) и другие события, в системном журнале аудита. Этот журнал обычно находится по адресу `/var/log/audit/audit.log`. Просматривать его можно также с помощью утилиты `journalctl`.
7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию? Для получения более конкретной информации о контекстах, связанных с FTP, можно использовать следующие команды: • Для просмотра существующих правил файловых контекстов: `semanage fcontext -l | grep ftp`. • Для просмотра булевых переключателей, влияющих на FTP: `semanage boolean -l | grep ftp`. • Чтобы узнать, какие типы (types) в политике SELinux существуют для FTP, можно использовать `seinfo -t | grep ftp`.
8. Сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать? Самый быстрый способ определить, является ли SELinux причиной проблемы, это временно перевести его в разрешающий режим (`permissive`) с помощью команды `setenforce 0`. После этого попробуйте снова запустить проблемный сервис. Если сервис начинает работать нормально, то проблема связана с

политикой SELinux. Не забудьте вернуть SELinux в принудительный режим (setenforce 1) после завершения диагностики.