Лабораторная работа №9

Артём Дмитриевич Петлин

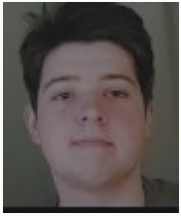
2025-11-01

Содержание i

1. Информация

1.1 Докладчик

- Петлин Артём Дмитриевич
- студент
- группа НПИбд-02-24
- Российский университет дружбы народов
- 1132246846@pfur.ru
- https://github.com/hikrim/study_2025-2026_os2



2. Цель работы

2.1 Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

3. Задание

3.1 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).

4. Теоретическое введение

SELinux (Security-Enhanced Linux) — реализация мандатного управления доступом в ядре Linux. Мандатное управление доступом (Mandatory Access Control, MAC) — разграничение прав доступа субъектов к объектам системы на базе меток конфиденциальности. Под объектами понимаются файлы, каталоги, устройства операционной системы. В качестве субъектов выступают процессы операционной системы. Метка в SELinux — контекст SELinux, содержащий информацию о принадлежности объекта системы пользователю SELinux, о его роли, типе и уровне безопасности. Основное назначение архитектуры MAC [5] — возможность принудительного назначения административно-установленной политики безопасности над всеми процессами и файлами системы. Политики безопасности SELinux работают поверх стандартного дискреционного управления контролем доступа (Discretionary Access Control, DAC) в Unix/Linux операционных системах.

5. Выполнение лабораторной работы

Получаем полномочия администратора. Просматриваем подробную информацию о текущем состоянии SELinux, анализируя вывод команды.

```
adpetlin@adpetlin:~$ su -
Password:
Last login: Sat Oct 25 22:41:11 MSK 2025 on pts/1
root@adpetlin:~# 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@adpetlin:~#
```

Рисунок 1: selinux

Проверяем текущий режим работы SELinux. Убеждаемся, что по умолчанию используется режим принудительного исполнения. Изменяем режим работы SELinux на разрешающий и подтверждаем изменение текущего режима.

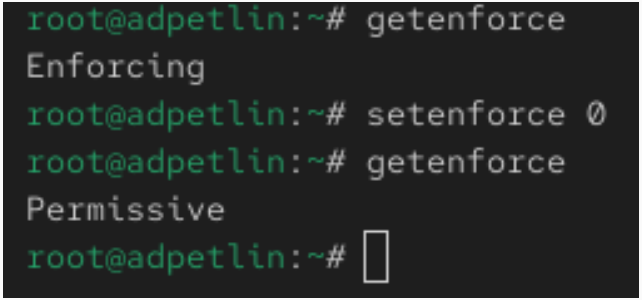


Рисунок 2: getenforce

```
#
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
```

Рисунок 3: disabled

Редактируем конфигурационный файл, чтобы полностью отключить SELinux, и перезагружаем систему.

```
adpetlin@adpetlin:~$ su -
Password:
Last login: Sat Nov  1 12:58:24 MSK 2025 on pts/0
root@adpetlin:~# getenforce
Disabled
root@adpetlin:~# setenforce 1
setenforce: SELinux is disabled
root@adpetlin:~#
```

Рисунок 4: getenforce

После перезагрузки снова проверяем статус SELinux и убеждаемся, что он отключен.

Пытаемся переключить режим работы SELinux без перезагрузки и анализируем реакцию системы.

```
SELINUX=enforcing
# 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
```

Рисунок 5: enforcing

Возвращаем настройку SELinux в режим принудительного исполнения через конфигурационный файл и перезагружаем систему. Во время загрузки наблюдаем сообщения системы, связанные с восстановлением меток безопасности.

После завершения загрузки проверяем, что система работает в принудительном режиме с активным SELinux.

```
adpetlin@adpetlin:~$ su -
Password:
Last login: Sat Nov  1 13:01:35 MSK 2025 on pts/0
root@adpetlin:~# 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@adpetlin:~#
```

Рисунок 6: setstatus -v

Получаем полномочия администратора. Просматриваем контекст безопасности системного файла. Копируем этот файл в домашний каталог и проверяем, как изменился его контекст безопасности. Перемещаем файл обратно в системный каталог, заменяя оригинал. Убеждаемся, что контекст безопасности файла остался неправильным. Восстанавливаем правильный контекст безопасности для файла с подробным выводом процесса. Проверяем, что контекст

```
root@adpetlin:~# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
root@adpetlin:~# cp /etc/hosts ~/
root@adpetlin:~# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
root@adpetlin:~# mv ~/hosts /etc
mv: overwrite '/etc/hosts'? yes
root@adpetlin:~# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
root@adpetlin:~# 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@adpetlin:~# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
root@adpetlin:~# touch /.autorelabel
root@adpetlin:~#
```

Рисунок 7: restorecon

5.8 Ход работы

Получаем полномочия администратора. Устанавливаем необходимое программное обеспечение: httpd и lynx.

Рисунок 8: httpd

Рисунок 9: lynx

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

Рисунок 10: web

Создаем новый каталог для файлов веб-сервера вне стандартного расположения. Создаем в этом каталоге тестовую веб-страницу.

Изменяем конфигурацию веб-сервера, указывая новый каталог в качестве корневого и настраивая правила доступа к нему. Запускаем веб-сервер и добавляем его в автозагрузку.

```
#DocumentRoot "/var/www/html"
DocumentRoot "/web"
```

Рисунок 11: DocumentRoot

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

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

Рисунок 12: Directory

Пытаемся обратиться к веб-серверу через текстовый браузер и обнаруживаем, что отображается стандартная страница, а не наша.

```
457  systemctl start httpd
458  systemctl enable httpd
```

Рисунок 13: lynx

Рисунок 14: Red Hat

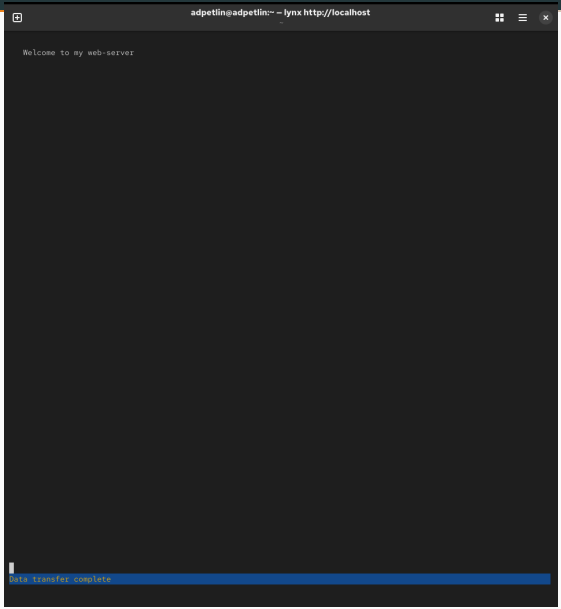
```
root@adpetlin:~# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
root@adpetlin:~# restorecon -R -v /web
Relabeled /web from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0
Relabeled /web/index.html from unconfined_u:object_r:default_t:s0 to unconfined_u:object_r:httpd_sys_content_t:s0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

Рисунок 15: semanage | restorecon

Добавляем правило в политику SELinux, назначая правильный тип контекста для нового каталога и его содержимого. Восстанавливаем контекст безопасности для нового каталога с рекурсивным применением.

5.13 Ход работы

Снова обращаемся к веб-серверу и убеждаемся, что теперь отображается наша пользовательская страница. При необходимости перезагружаем систему.



Получаем полномочия администратора. Просматриваем список всех переключателей SELinux, связанных со службой FTP.

```
adpetlin@adpetlin:~$ su -
Password:
Last login: Sat Nov  1 13:14:12 MSK 2025 on pts/0
root@adpetlin:~# 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@adpetlin:~#
```

Рисунок 17: getsebool

Ищем подробное описание переключателей для анонимного доступа FTP, включая их текущее состояние и назначение. Временно изменяем значение одного из переключателей. Проверяем, что значение переключателя изменилось. Снова смотрим подробный список переключателей и обращаем внимание на разницу между временным и постоянным состоянием. Изменяем значение переключателя постоянно. Проверяем окончательное состояние переключателя, убеждаясь, что теперь и временное, и постоянное значения совпадают.

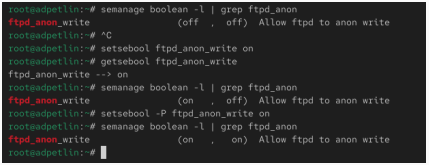


Рисунок 18: setsebool

6. Выводы

6.1 Выводы

Мы получили навыки работы с контекстом безопасности и политиками SELinux.

Список литературы

Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009.
2. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
3. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — (Системный администратор).
4. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер,
5. — (Классика Computer Science).
6. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
7. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Indepen- dently published, 2017.
8. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.