

# Лабораторная работа №9.

## Управление SELinux

---

Жукова А.А

31 октября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

# Докладчик

---

- Жукова Арина Александровна
- Студент бакалавриата, 2 курс
- группа: НПИбд-03-23
- Российский университет дружбы народов
- 1132239120@rudn.ru



## Вводная часть

---

## Цель работы

---

Лабораторная работа направлена на получение навыков работы с контекстом безопасности и политиками SELinux.

## Задание

---

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

## Результаты и анализ лабораторной работы

---

# Управление режимами SELinux

1. Для просмотра текущей информации о состоянии SELinux используем `sestatus -v`

```
[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# 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/getty                      system_u:object_r:getty_exec_t:s0
```

### 2. Изменение режима работы SELinux на разрешающий (Permissive)

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

- Попробовали переключить режим работы SELinux: `setenforce 1`. Не могла переключаться между отключённым и принудительным режимом без перезагрузки системы.

```
[aazhukoval@aazhukoval ~]$ su -
Пароль:
[root@aazhukoval ~]# getenforce
Disabled
[root@aazhukoval ~]# setenforce 1
setenforce: SELinux is disabled
[root@aazhukoval ~]# █
```

## Использование restorecon для восстановления контекста безопасности

1. Просмотр контекста безопасности файла /etc/hosts: ls -Z /etc/hosts.

```
[root@aazhukova1 ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@aazhukova1 ~]# cp /etc/hosts ~/
[root@aazhukova1 ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@aazhukova1 ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'? y
[root@aazhukova1 ~]# ls -Z /etc/hosts
unconfined_u:object_r:admin_home_t:s0 /etc/hosts
[root@aazhukova1 ~]#
```

## Использование restorecon для восстановления контекста безопасности

2. Исправление контекста безопасности `restorecon -v /etc/hosts`. Опция `-v` показала процесс изменения. Убедилась, что тип контекста изменился. Для массового исправления контекста безопасности на файловой системе используем `touch /.autorelabel`.

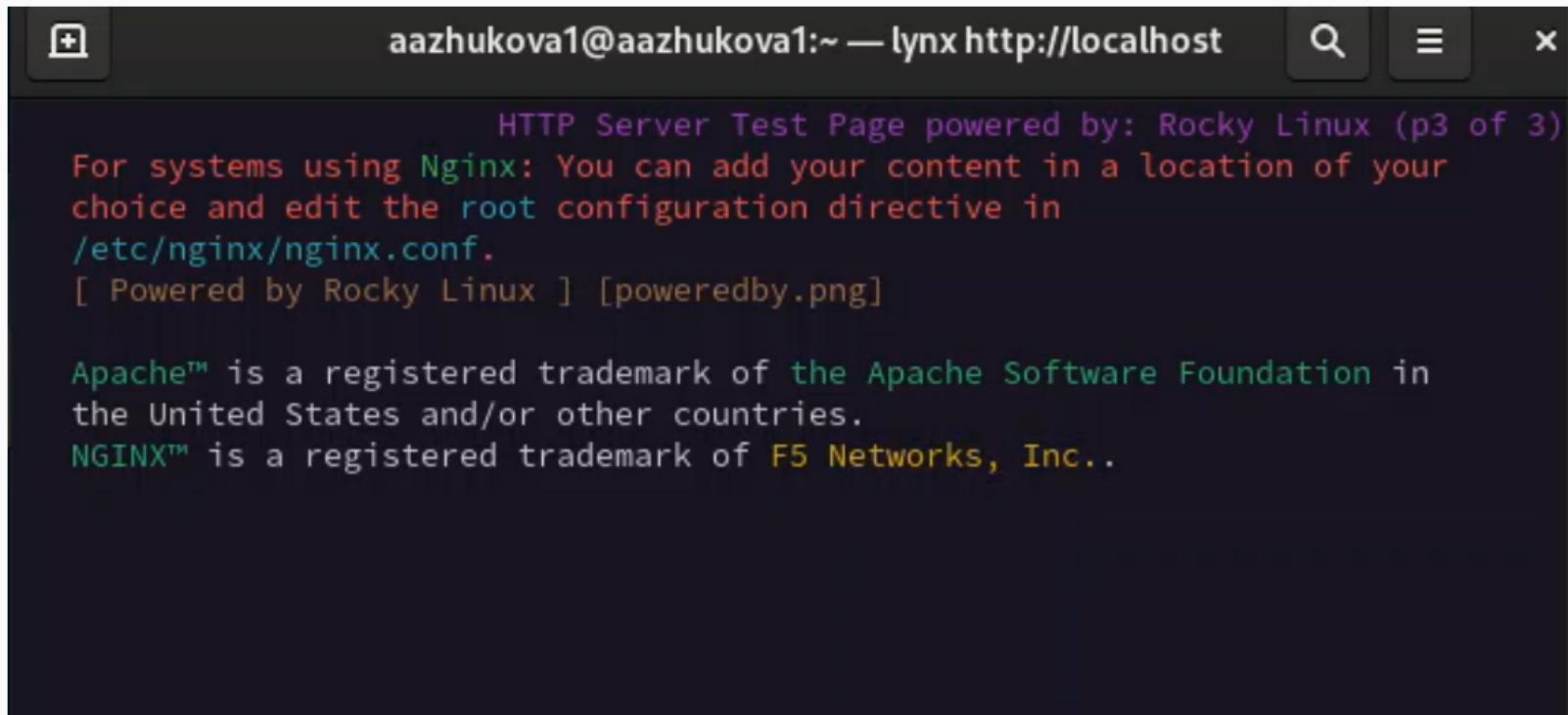
```
[root@aazhukova1 ~]# restorecon -v /etc/hosts
Relabeled /etc/hosts from unconfined_u:object_r:admin_home_t:s0 to unconfined_u:object_r:net_c
onf_t:s0
[root@aazhukova1 ~]# ls -Z /etc/hosts
unconfined_u:object_r:net_conf_t:s0 /etc/hosts
[root@aazhukova1 ~]# touch /.autorelabel
[root@aazhukova1 ~]#
```

1. Запуск веб-сервера и службы httpd.

```
[root@aazhukova1 ~]# systemctl start httpd
[root@aazhukova1 ~]# systemctl enable httpd
[root@aazhukova1 ~]#
```

## Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

2. В терминале под учётной записью своего пользователя обращаемся к веб-серверу в текстовом браузере lynx: `lynx http://localhost`.



The screenshot shows a terminal window with the following content:

```
aazhukova1@aazhukova1:~ — lynx http://localhost
```

HTTP Server Test Page powered by: Rocky Linux (p3 of 3)  
For systems using Nginx: You can add your content in a location of your  
choice and edit the root configuration directive in  
`/etc/nginx/nginx.conf`.  
[ Powered by Rocky Linux ] [poweredby.png]

Apache™ is a registered trademark of the Apache Software Foundation in  
the United States and/or other countries.  
NGINX™ is a registered trademark of F5 Networks, Inc..

11/16

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

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

## Работа с переключателями SELinux

1. Вывод списка переключателей SELinux для службы ftp: `getsebool -a | grep ftp`.

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

## Работа с переключателями SELinux

2. Изменение текущего значения переключателя для службы ftpd\_anon\_write с off на on.

```
[root@aazhukova1 ~]# setsebool ftpd_anon_write on
[root@aazhukova1 ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@aazhukova1 ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write           (вкл. ,выкл.)  Allow ftpd to anon write
[root@aazhukova1 ~]#
```

3. Изменение постоянного значение переключателя для службы ftpd\_anon\_write с off на on: `setsebool -P ftpd_anon_write on`.

```
[root@aazhukova1 ~]# setsebool -P ftpd_anon_write on  
  
[root@aazhukova1 ~]#  
[root@aazhukova1 ~]# semanage boolean -l | grep ftpd_anon  
ftpd_anon_write          (вкл. , вкл.)  Allow ftpd to anon write  
[root@aazhukova1 ~]#
```

## Выводы

---

## Выводы

---

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