Отчет по лабораторной работе №9

SELinux

Власов А.С

1 ноября 2025

Российский университет дружбы народов, Москва, Россия

- Власов Артем Сергеевич

- студент НПИбд-01-24

- номер студ. билета 1132246841

- Российский университет дружбы народов

- 1132246841@pfur.ru

Цели и задачи

Получить навыки работы с контекстом безопасности и политивами SELinux

Продемонстрировать навыки умения работать с SELinux.

Выполнение лабораторной работы

Получаем текущую информацию о состоянии SELinux.

Рис. 1: Статус SELinux

В файле конфигурации задаем значение disabled и перезапускаем систему.

```
19 #
20 #      grubby --update-kernel ALL --remove-args selinux
21 #
22 SELINUX=disabled
23 # SELINUXTYPE- can take one of these three values:
```

Рис. 2: Отключение

Возвращаем статус enforcing и снова перезагружаем систему.

```
19 #
20 #     grubby --update-kernel ALL --remove-args selinux
21 #
22 SELINUX=enforcing
23 # SELINUXTYPE= can take one of these three values:
```

Рис. 3: Проверка события

```
[root@asvlasov ~]# setenforce 1
[root@asvlasov ~]# getenforce
Enforcing
[root@asvlasov ~]# 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
```

Начинаем работу с контекстом безопасности.

Рис. 5: Работа с контекстом

Рис. 6: Перемаркировка

В файле который мы создали вводим строчку. Меняем конфигурацию.

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

Открыть ▼ | ⊞

index.h
/web

1 Welcome to my web server
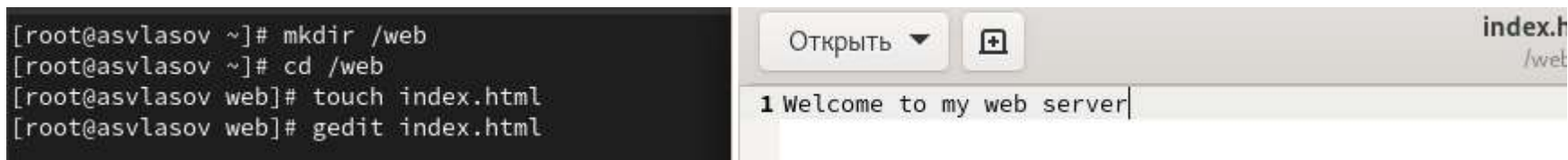
Рис. 7: index

```
# 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. 8: Конфигурация

Начинаем работу с переключателями.

Рис. 9: Работа с переключателями

Выводы

Мы научились работать с контекстом безопасности и политивами SELinux.