## Лабораторная работа №9

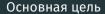
Управление SELinux

Эзиз Хатамов

16 октября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы



Получить навыки работы с контекстом безопасности и политиками SELinux.

Ход выполнения работы

## Управление режимами SELinux

```
ehatamov@ehatamov:~$ su
Password:
root@ehatamov:/home/ehatamov# sestatucs -v
bash: sestatucs: command not found...
root@ehatamov:/home/ehatamov# sestatus -v
SELinux status:
                                enabled
SELinuxfs mount:
                                /svs/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
                                actual (secure)
Memory protection checking:
Max kernel policy version:
                                33
Process contexts:
Current context:
                                unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023
                                svstem_u:system_r:init_t:s0
Init context:
/usr/sbin/sshd
                                system u:system r:sshd t:s0-s0:c0.c1023
File contexts:
Controlling terminal:
                                unconfined u:object r:user devots 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@ehatamov:/home/ehatamov# getenforce
Enforcing
root@ehatamov:/home/ehatamov# setenforce 0
root@ehatamov:/home/ehatamov# getenforce
Parmicciva
root@ehatamov:/home/ehatamov#
```

## Восстановление контекста безопасности

- · Копирование файла изменяет контекст на admin\_home\_t
- Восстановление корректного типа:
  - restorecon -v /etc/hosts

Рис. 2: Восстановление контекста безопасности

## Настройка контекста безопасности веб-сервера

- · В конфигурации Apache изменён DocumentRoot на /web
- Применён контекст httpd\_sys\_content\_t:



Рис. 3: Работа пользовательского веб-сервера

· Изменение параметра ftpd\_anon\_write с off на on

```
ehatamov@ehatamov:~$ lynx http://localhost
ehatamov@ehatamov:~$
ehatamov@ehatamov:~$ su
Password:
root@ehatamov:/home/ehatamov#
root@ehatamov:/home/ehatamov# 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@ehatamov:/home/ehatamov# semanage boolean -l | grep ftpd anon
ftpd anon write
                               (off . off) Allow ftpd to anon write
root@ehatamov:/home/ehatamov# setsebool ftpd anon write on
root@ehatamov:/home/ehatamov# getsebool ftpd anon write
ftpd anon write --> on
root@ehatamov:/home/ehatamov# semanage boolean -l | grep ftpd anon
ftpd anon write
                               (on . off) Allow ftpd to anon write
root@ehatamov:/home/ehatamov# setsebool -P ftpd anon write on
```

Итоги работы \_\_\_\_\_\_

- · Изучены принципы функционирования SELinux и его режимы (Enforcing, Permissive, Disabled)
- Выполнена настройка контекста безопасности для нестандартного каталога веб-сервера
- · Изучены инструменты semanage, restorecon, setsebool и getsebool
- · Освоены методы управления контекстами и политиками безопасности в Linux