

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# sestatus -v
bash: sestatus: command not found...
root@ehatamov:/home/ehatamov# 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@ehatamov:/home/ehatamov# getenforce
Enforcing
root@ehatamov:/home/ehatamov# setenforce 0
root@ehatamov:/home/ehatamov# getenforce
Permissive
root@ehatamov:/home/ehatamov#
```

- Копирование файла изменяет контекст на `admin_home_t`
- Восстановление корректного типа:
 - `restorecon -v /etc/hosts`

```
[ 0.717674] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 0.717676] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 0.717677] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 5.812741] selinux-autorelabel[833]: *** Warning -- SELinux targeted policy relabel is required.
[ 5.812888] selinux-autorelabel[833]: *** Relabeling could take a very long time, depending on file
[ 5.812829] selinux-autorelabel[833]: *** system size and speed of hard drives.
[ 5.815203] selinux-autorelabel[833]: Running: /sbin/fixfiles -T 0 restore
```

Рис. 2: Восстановление контекста безопасности

- 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