

# Отчет по лабораторной работе 9

## SELinux

Власов Артем Сергеевич

### Содержание

1. Цель работы.....	1
2. Задание.....	1
3. Выполнение лабораторной работы 9.....	1
4. Выводы.....	4
Список литературы.....	4

### 1. Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux

### 2. Задание

Продемонстрировать навыки умения работать с SELinux.

### 3. Выполнение лабораторной работы 9.

Получаем текущую информацию о состоянии SELinux.

```
[root@asvlasov ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current modes:                  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:rlogin_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@asvlasov ~]# getenforce
Enforcing
[root@asvlasov ~]# setenforce 0
[root@asvlasov ~]# getenforce
Permissive
[root@asvlasov ~]#
```

Статус SELinux

По умолчанию он находится в режиме enforcing переводим его в режим permissive.

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:
```

## Отключение

Видим, что SELinux отключен.

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:
```

## Включение

```
[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
[root@asvlasov ~]#
```

## Проверка статуса

Начинаем работу с контекстом безопасности.

```
[root@asvlasov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@asvlasov ~]# cp /etc/hosts ~/
[root@asvlasov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@asvlasov ~]# mv ~/hosts /etc
mv: переписать '/etc/hosts'?
[root@asvlasov ~]# ls -Z ~/hosts
unconfined_u:object_r:admin_home_t:s0 /root/hosts
[root@asvlasov ~]# restorecon -v /etc/hosts
[root@asvlasov ~]# ls -Z /etc/hosts
system_u:object_r:net_conf_t:s0 /etc/hosts
[root@asvlasov ~]# touch /.autorelabel
[root@asvlasov ~]#
```

## Работа с контекстом


Копируем файл с меткой контекста в домашний каталог, видим, что метка изменилась. Перезапишем и увидим что контекст не изменился, затем исправляем контекст безопасности, и видим что все вернулось в значение по умолчанию. Запускаем массовое исправление контекстов и видим что система была перемаркирована после перезагрузки

```
[ 0.291751] Warning: Deprecated Hardware is detected: x86_64-v2:AuthenticAMD:
AMD Ryzen 5 5500U with Radeon Graphics will not be maintained in a future major
release and may be disabled
[ 3.261610] systemd[1]: Invalid DMI field header.
[ 4.873260] Warning: Unmaintained driver is detected: e1000
[ 5.784387] vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on
an unsupported hypervisor.
[ 5.784398] vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely b
roken.
[ 5.784404] vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported g
raphics device to avoid problems.
[ 14.143080] selinux-autorelabel[763]: *** Warning -- SELinux targeted policy relabel is required.
[ 14.143489] selinux-autorelabel[763]: *** Relabeling could take a very long time, depending on file
[ 14.143600] selinux-autorelabel[763]: *** system size and speed of hard drives.
[ 14.167907] selinux-autorelabel[763]: Running: /sbin/fixfiles -T 0 restore
[ 28.000499] selinux-autorelabel[769]: Warning: Skipping the following R/O filesystems:
[ 28.001591] selinux-autorelabel[769]: /run/credentials/systemd-sysctl.service
[ 28.001751] selinux-autorelabel[769]: /run/credentials/systemd-tmpfiles-setup-dev.service
[ 28.001855] selinux-autorelabel[769]: /run/credentials/systemd-tmpfiles-setup.service
[ 28.001947] selinux-autorelabel[769]: Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev
/lddebug /sys/kernel/tracing
/
```

## Перемаркировка

В файле который мы создали вводим строчку.

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

Открыть  index.t  
/web

1 Welcome to my web server|

## index

Далее меняем файл конфигурации добавляя путь к нашей созданной директории.

```
..
# 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>
```

## Конфигурация

Начинаем работу с переключателями.

```

[root@asvlasov ~]# 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@asvlasov ~]# semanage boolean -l | grep ftpd_anon
bash: grepftpd_anon: команда не найдена...
BrokenPipeError: [Errno 32] Broken pipe
[root@asvlasov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (выкл.,выкл.) Allow ftpd to anon write
[root@asvlasov ~]# setsebool ftpd_anon_write on
[root@asvlasov ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@asvlasov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. ,выкл.) Allow ftpd to anon write
[root@asvlasov ~]# setsebool -P ftpd_anon_write on
[root@asvlasov ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write (вкл. , вкл.) Allow ftpd to anon write
[root@asvlasov ~]#

```

### *Работа с переключателями*

Смотрим список всех переключателей службы ftp, затем для ftpd\_anon. Меняем значение переключателя на on. Смотрим изменения, далее ставим флаг on для другого переключателя.

## 4. Выводы

Мы научились работать с контекстом безопасности и политиками SELinux

## Список литературы