Лабораторная работа

Номер 9

Приходько Иван Иванович

27 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Приходько Иван Иванович
- Студент
- Российский университет дружбы народов

Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

Задание

Поработать с контекстом безопасности и политиками SELinux.

Работа с SELinux

Для начала посмотрим статус SELinux

```
[root@ivanprihodko cron.d]# 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_exe
c_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@ivanprihodko cron.d]# getenforce
Enforcing
```

Работа с SELinux

Теперь в файле отключим SELinux

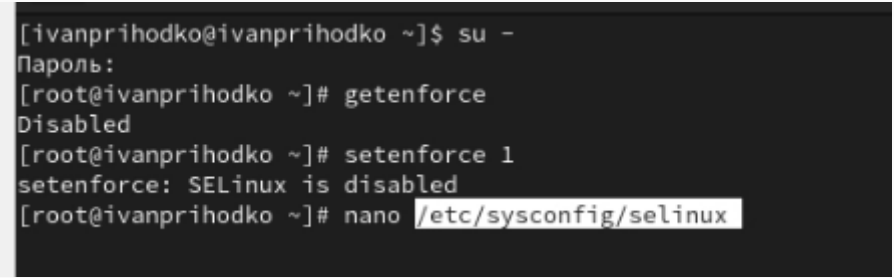
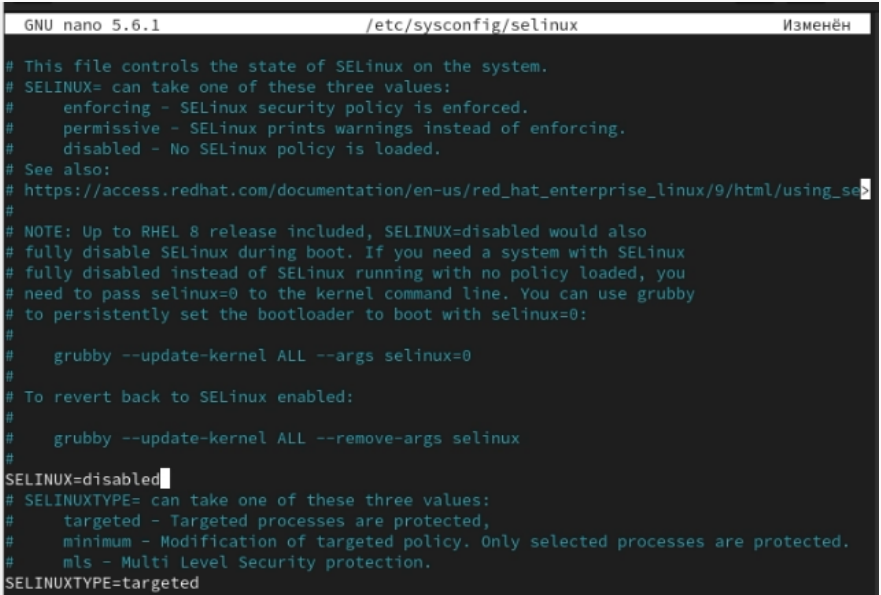


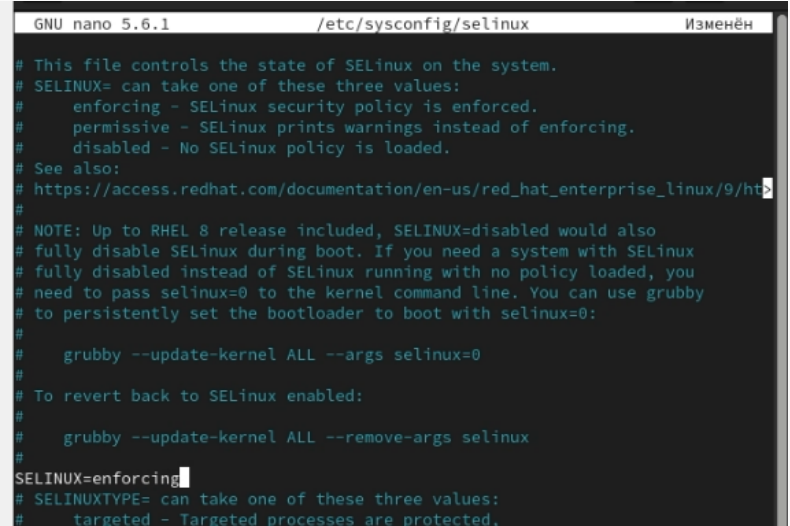
Рис. 2: ОТключение SELinux

Работа с SELinux



Работа с SELinux

Теперь вернем SELinux в enforcing



Работа с SELinux

После перезапусками системы SELinux снова включен

```
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# 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:c
0.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@ivanprihodko ~]# getenforce
Enforcing
[root@ivanprihodko ~]# ls -Z /etc/hosts
```

Теперь поработаем с контекстом безопасности файла

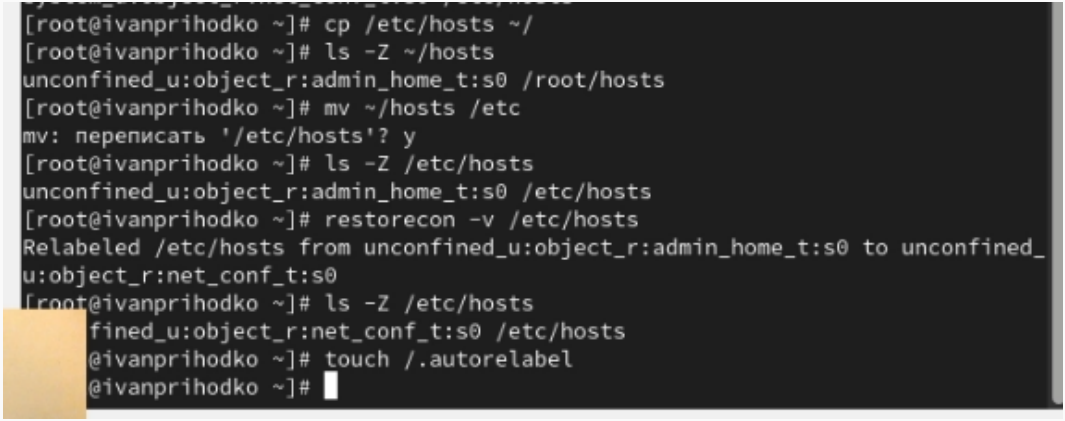


Рис. 6: Работа с контекстом безопасности файла

Далее добавим пару строк в httpd.conf

Работа с SELinux

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
#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>
```

Теперь запустим httpd

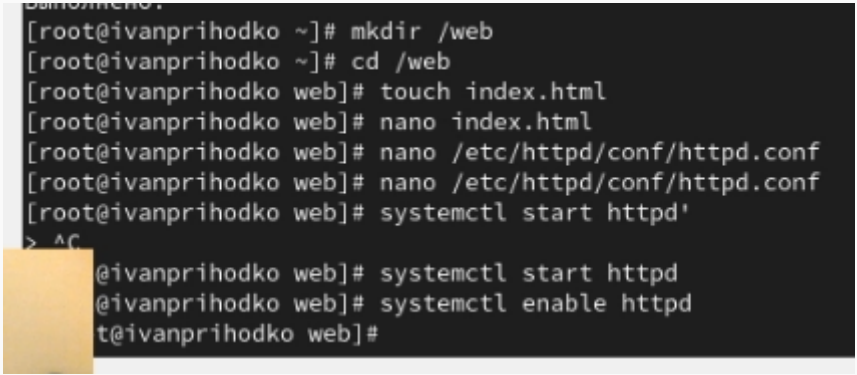


Рис. 9: Запуск httpd

Работа с SELinux

Поработаем немного с httpd и выведем список переключатей SELinux

```
[root@ivanprihodko web]# systemctl start httpd
[root@ivanprihodko web]# systemctl enable httpd
\[root@ivanprihodko web]# lynx http://localhost
[root@ivanprihodko web]# su - ivanprihodko
[ivanprihodko@ivanprihodko ~]$ lynx http://localhost
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?
"
[root@ivanprihodko ~]# 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 unconfine
d_u:object_r:httpd_sys_content_t:s0
[root@ivanprihodko ~]# su - ivanprihodko
[ivanprihodko@ivanprihodko ~]$ lynx http://localhost
[ivanprihodko@ivanprihodko ~]$ 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
[ivanprihodko@ivanprihodko ~]$ semanage boolean -l | grep ftpd_anon
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
```

Работа с SELinux

Теперь поработаем с переключателями SELinux

```
[ivanprihodko@ivanprihodko ~]$ semanage boolean -l | grep ftpd_anon
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[ivanprihodko@ivanprihodko ~]$ setsebool ftpd_anon_write on
Could not change active booleans. Please try as root: Permission denied
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
[root@ivanprihodko ~]# 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@ivanprihodko ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (выкл.,выкл.)  Allow ftpd to anon write
[root@ivanprihodko ~]# setsebool ftpd_anon_write on
[root@ivanprihodko ~]# getsebool ftpd_anon_write
ftpd_anon_write --> on
[root@ivanprihodko ~]# semanage boolean -l | grep ftpd_anon
ftpd_anon_write                (вкл. ,выкл.)  Allow ftpd to anon write
[root@ivanprihodko ~]# setsebool -P ftpd_anon_write on
```

Выводы

В ходе данной работы были получены навыки для работы с контекстом безопасности и политиками SELinux.