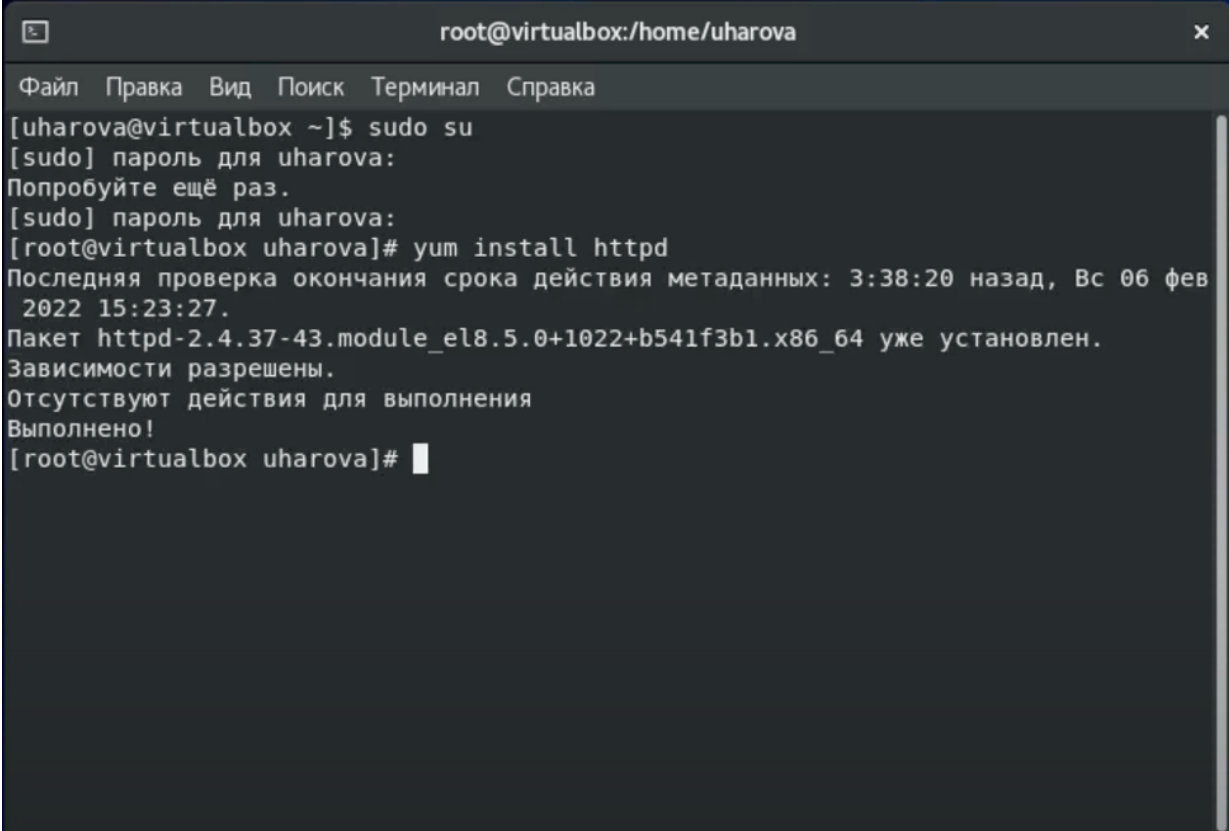


Лабораторная 6

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Установим httpd



```
root@virtualbox:/home/uharova
Файл  Правка  Вид  Поиск  Терминал  Справка
[uharova@virtualbox ~]$ sudo su
[sudo] пароль для uharova:
Попробуйте ещё раз.
[sudo] пароль для uharova:
[root@virtualbox uharova]# yum install httpd
Последняя проверка окончания срока действия метаданных: 3:38:20 назад, Вс 06 фев 2022 15:23:27.
Пакет httpd-2.4.37-43.module_el8.5.0+1022+b541f3b1.x86_64 уже установлен.
Зависимости разрешены.
Отсутствуют действия для выполнения
Выполнено!
[root@virtualbox uharova]#
```

{ #fig:001 width=70% }

Вносим изменения в конфигурационный файл

```
[root@virtualbox uharova]# echo "ServerName test.ru" >> /etc/httpd/httpd.conf
[root@virtualbox uharova]# cat /etc/httpd/httpd.conf
ServerName test.ru
Listen 80
ServerName test.ru
[root@virtualbox uharova]#
```

{ #fig:002 width=70% }

Убедимся, что SELinux работает в нужном режиме, а также найдем apache в списке процессов

```
[root@virtualbox uharova]# iptables -F
[root@virtualbox uharova]# iptables -P INPUT ACCEPT
[root@virtualbox uharova]# iptables -P OUTPUT ACCEPT
[root@virtualbox uharova]# getenforce
Enforcing
[root@virtualbox uharova]# sestatus
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
```

{ #fig:003 width=70% }

Посмотрим состояние переключателей

```
root@virtualbox:/home/uharova
Файл Правка Вид Поиск Терминал Справка
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_opencryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
[root@virtualbox uharova]# ch
```

{ #fig:004 width=70% }

Просмотрим статистику по политике

```
root@virtualbox:/home/uharova
Файл Правка Вид Поиск Терминал Справка
Policy Version: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 463
Sensitivities: 1 Categories: 1024
Types: 4959 Attributes: 255
Users: 8 Roles: 14
Booleans: 340 Cond. Expr.: 389
Allow: 112894 Neverallow: 0
Auditallow: 166 Dontaudit: 10362
Type_trans: 253622 Type_change: 87
Type_member: 35 Range_trans: 6015
Role_allow: 38 Role_trans: 423
Constraints: 72 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 0 Polcap: 5
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 33
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0
[root@virtualbox uharova]#
```

{ #fig:005 width=70% }

Определим тип файлов и поддиректорий

```
[root@virtualbox uharova]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 27 21
:47 html
[root@virtualbox uharova]#
```

{ #fig:006 width=70% }

Проверим, работает ли Веб-сервер, и запустим его

```
[root@virtualbox uharova]# chcon -t samba_share_t /var/www/html/test.html
[root@virtualbox uharova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@virtualbox uharova]# sestatus
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
[root@virtualbox uharova]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@virtualbox uharova]# service httpd sta
```

{ #fig:007 width=70% }

Пробуем перейти по ссылке и получаем ошибку доступа

{ #fig:008 width=70% }

Просмотрим права доступа и лог

```
root@virtualbox:/home/uharova
Файл  Правка  Вид  Поиск  Терминал  Справка
Feb  6 20:03:54 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:03:59 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:02 virtualbox org.gnome.Shell.desktop[2302]: Window manager warning
: last_user_time (103574118) is greater than comparison timestamp (103574087).
This most likely represents a buggy client sending inaccurate timestamps in mess
ages such as _NET_ACTIVE_WINDOW.  Trying to work around...
Feb  6 20:04:02 virtualbox org.gnome.Shell.desktop[2302]: Window manager warning
: W94 appears to be one of the offending windows with a timestamp of 103574118.
Working around...
Feb  6 20:04:04 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:09 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:14 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:19 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:24 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
Feb  6 20:04:29 virtualbox kernel: VBGL_IOCTL_ACQUIRE_GUEST_CAPABILITIES failed
rc=-138
[root@virtualbox uharova]#
```

{ #fig:009 width=70% }

Пробуем запустить веб-сервер на прослушивание TCP-порта 81

 { #fig:010 width=70% }

И пробуем снова открыть веб-страницу

 { #fig:011 width=70% }

Откроем веб-страницу через порт 81

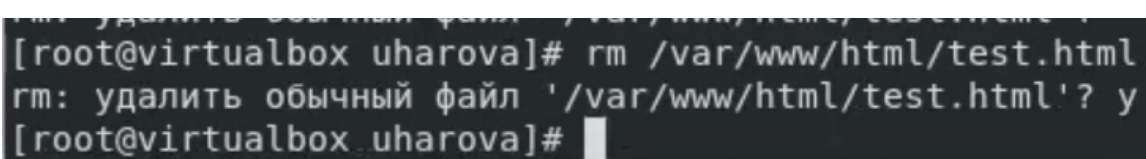
 { #fig:012 width=70% }

Удалим привязку к 81 порту

```
ServerName test.ru
Listen 80
```

{ #fig:013 width=70% }

Удалим файл test.html

A terminal window screenshot showing the command 'rm /var/www/html/test.html' being executed. The prompt is '[root@virtualbox uharova]#'. The output shows a confirmation message: 'rm: удалить обычный файл '/var/www/html/test.html'? y'. The prompt returns to '[root@virtualbox uharova]#'.

```
[root@virtualbox uharova]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@virtualbox uharova]#
```

{ #fig:014 width=70% }

Вывод

В результате проделанной работы мы приобрели навыки администрирования ОС Linux и проверили работу SELinux на практике совместно с веб-сервером Apache.