

Лабораторная работа №6

Мандатное разграничение прав в Linux атрибутов

Victoria M. Shutenko

15 October, 2022, Moscow, Russian Federation

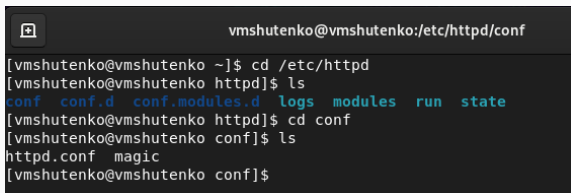
RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной
работы

Цель выполнения лабораторной работы

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

Результаты выполнения лабораторной работы

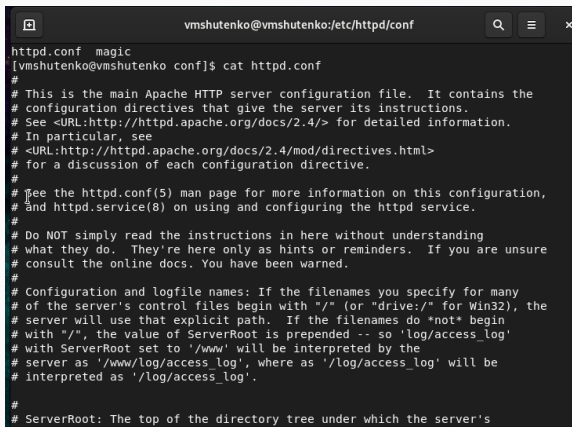


```
vmshutenko@vmshutenko:/etc/httpd/conf

[vmshutenko@vmshutenko ~]$ cd /etc/httpd
[vmshutenko@vmshutenko httpd]$ ls
conf  conf.d  conf.modules.d  logs  modules  run  state
[vmshutenko@vmshutenko httpd]$ cd conf
[vmshutenko@vmshutenko conf]$ ls
httpd.conf  magic
[vmshutenko@vmshutenko conf]$
```

Figure 1: Установка httpd.

Подготовка к выполнению лабораторной работы №6

A terminal window with a dark background. The title bar shows the user 'vmshutenko' at host 'vmshutenko' in the directory '/etc/httpd/conf'. The terminal displays the output of the 'cat httpd.conf' command. The file content is a configuration file for the Apache HTTP server, starting with a magic number and followed by several comment lines explaining the file's purpose and usage. The comments include instructions on how to use the file, where to find more information, and warnings about not simply reading the instructions without understanding them. The file also mentions the 'ServerRoot' directory and the 'log/access_log' file.

```
vmshutenko@vmshutenko:/etc/httpd/conf
httpd.conf magic
[vmshutenko@vmshutenko conf]$ cat httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
```

Figure 2: Файл httpd.conf.

```
root@vmshutenko:~# cat /etc/passwd | grep vmshutenko
vmshutenko:vmshutenko:0:0:vmshutenko:/home/vmshutenko:/bin/bash
[vmshutenko@vmshutenko conf]$ su root
Пароль:
[root@vmshutenko conf]# echo "ServerName test.ru" >> httpd.conf
[root@vmshutenko conf]#
```

Figure 3: Задание параметра ServerName

Подготовка к выполнению лабораторной работы №6

```
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName test.ru
[root@vmshutenko conf]#
```

Figure 4: Проверка наличия параметра ServerName


```
[root@vmshutenko vmshutenko]# iptables -F
[root@vmshutenko vmshutenko]# iptables -P INPUT ACCEPT iptables -p OUTPUT ACCEPT
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
[root@vmshutenko vmshutenko]# iptables -P INPUT ACCEPT
[root@vmshutenko vmshutenko]# iptables -P OUTPUT ACCEPT
```

Figure 5: Отключение пакетного фильтра.

```
[root@vmshutenko vmshutenko]# getenforce
Enforcing
[root@vmshutenko vmshutenko]# setstatus
bash: setstatus: command not found...
[root@vmshutenko vmshutenko]# 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@vmshutenko vmshutenko]#
```

Figure 6: Проверка работоспособности SELinux.

Проверка работоспособности веб-сервера с помощью браузера

```
[root@vmshutenko vmshutenko]# service httpd status
Redirecting to /bin/systemctl status httpd.service
○ httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pr
   Active: inactive (dead)
   Docs: man:httpd.service(8)
lines 1-4/4 (END)
```

Figure 7: Обращение к веб-серверу.

```
root@vmshutenko vmshutenko]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 2842 0.0 0.1 221688
2428 pts/0 S+ 17:41 0:00 grep --color=auto httpd
root@vmshutenko vmshutenko]#
```

Figure 8: Определение контекста безопасности.

Текущее состояние переключателей SELinux для Apache

```
[root@vmshutenko vmshutenko]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.

Without options, show SELinux status.
[root@vmshutenko vmshutenko]# seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] y

* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
setools-console-4.4.0-5.el9.x86_64      Policy analysis command-line tools for SELinux
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
```

Figure 9: Определение текущего состояния переключателей SELinux.

```
[root@vmshutenko vmshutenko]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      133      Permissions:      454
Sensitivities: 1       Categories:       1024
Types:        5049     Attributes:       254
Users:        8       Roles:           14
Booleans:     347     Cond. Expr.:     380
Allow:        64620    Neverallow:      0
Auditallow:   168     Dontaudit:       8474
Type_trans:   258620  Type_change:     87
Type_member:  35      Range_trans:     5960
Role allow:   38      Role_trans:      420
Constraints:  72      Validatetrans:   0
MLS Constrai: 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:         653
Netifcon:     0      Nodecon:         0
```

Figure 10: Статистика по политике.

Определение типов файлов и поддиректорий, находящихся в директории /var/www и в директории /var/www/html:

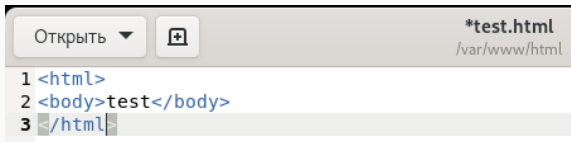
```
[root@vmshutenko vmshutenko]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июл 22 14
:43 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июл 22 14
:43 html
[root@vmshutenko vmshutenko]# ls -lZ /var/www/html
итого 0
[root@vmshutenko vmshutenko]#
```

Figure 11: Определение типов файлов и поддиректорий.

Круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[root@vmshutenko vmshutenko]# cd /var/www/html
[root@vmshutenko html]# ls -l
итого 0
[root@vmshutenko html]# cd /var/www
[root@vmshutenko www]# ls -l
итого 0
drwxr-xr-x. 2 root root 6 июл 22 14:43 cgi-bin
drwxr-xr-x. 2 root root 6 июл 22 14:43 html
[root@vmshutenko www]#
```

Figure 12: Определение круга пользователей.

A screenshot of a code editor window. The title bar at the top shows a button labeled "Открыть" (Open) with a dropdown arrow, a plus icon in a square, and the file name "*test.html" with the path "/var/www/html" below it. The editor area contains three lines of code: line 1 is "<html>", line 2 is "<body>test</body>", and line 3 is "</html>". The code is syntax-highlighted in blue. The background of the editor has alternating light and dark horizontal stripes.

```
1 <html>
2 <body>test</body>
3 </html>
```

Figure 13: Файл test.html.

Проверка, изменение и просмотр контекста

```
[root@vmshutenko html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@vmshutenko html]# chcon -t samba_share_t /var/www/html/test.html
[root@vmshutenko html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@vmshutenko html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 15 18:02 /var/www/html/test.html
[root@vmshutenko html]#
```

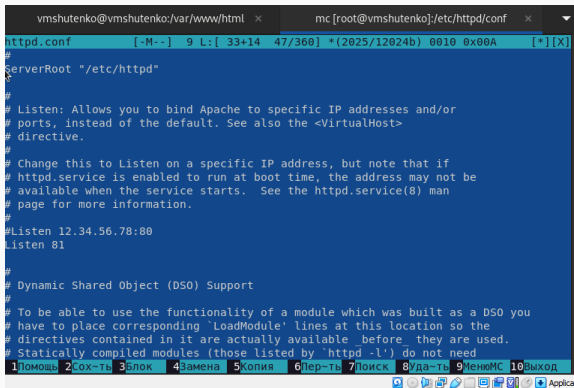
Figure 14: Проверка, изменение и просмотр контекста.

Просмотр log-файлов веб-сервера Apache.

```
[root@vmshutenko html]# tail /var/log/messages
Oct 15 18:09:14 vmshutenko systemd[1583]: Started Portal service (GTK/GNOME implemen
tation).
Oct 15 18:09:15 vmshutenko systemd[1583]: Started Portal service.
Oct 15 18:09:20 vmshutenko rtkit-daemon[732]: Successfully made thread 3810 of proce
ss 3682 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
Oct 15 18:09:45 vmshutenko journal[3745]: Failed to get application states: GDBus.Er
ror:org.freedesktop.portal.Error.Failed: Could not get window list
Oct 15 18:10:45 vmshutenko firefox.desktop[3682]: Missing chrome or resource URL: re
source://gre/modules/UpdateListener.jsm
Oct 15 18:10:45 vmshutenko firefox.desktop[3682]: Missing chrome or resource URL: re
source://gre/modules/UpdateListener.sys.mjs
Oct 15 18:16:27 vmshutenko gnome-shell[1690]: Window manager warning: last_user_time
(5598418) is greater than comparison timestamp (5598413). This most likely represe
nts a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WIN
DOW. Trying to work around...
Oct 15 18:16:27 vmshutenko gnome-shell[1690]: Window manager warning: W5 appears to
be one of the offending windows with a timestamp of 5598418. Working around...
Oct 15 18:16:29 vmshutenko gnome-shell[1690]: Window manager warning: last_user_time
(5600465) is greater than comparison timestamp (5600463). This most likely represe
nts a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WIN
DOW. Trying to work around...
Oct 15 18:16:29 vmshutenko gnome-shell[1690]: Window manager warning: W5 appears to
be one of the offending windows with a timestamp of 5600465. Working around...
```

Figure 15: Системный лог-файл.

Изменение Listen 80 на Listen 81 в файле httpd.conf.



```
vmshutenko@vmshutenko:/var/www/html x mc [root@vmshutenko]:/etc/httpd/conf x
httpd.conf [-M--] 9 L:[ 33+14 47/360] *(2025/12024b) 0010 0x00A [*][X]
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
1Помощь 2Сох-ть 3Блок 4Замена 5Копия 6Пер-ть 7Поиск 8Да-ть 9УенюМС 10Выход
```

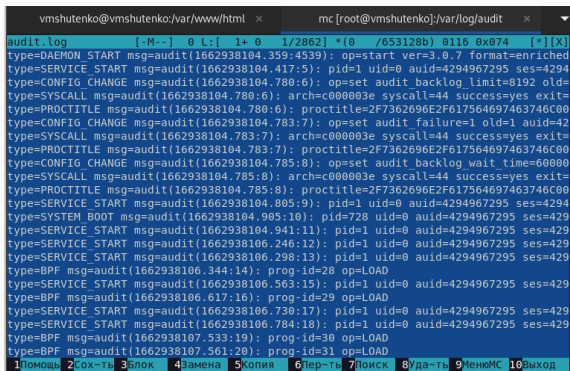
Figure 16: Изменение Listen 80 на Listen 81 в файле httpd.conf.

Просмотр лог-файлов:

```
DOW. Trying to work around...
Oct 15 18:16:29 vmshutenko gnome-shell[1690]: Window manager warning: W5 appears to
be one of the offending windows with a timestamp of 5600465. Working around...
[root@vmshutenko html]# tail /var/log/messages
Oct 15 18:16:27 vmshutenko gnome-shell[1690]: Window manager warning: last user time
(5598418) is greater than comparison timestamp (5598413). This most likely represe
nts a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WIN
DOW. Trying to work around...
Oct 15 18:16:27 vmshutenko gnome-shell[1690]: Window manager warning: W5 appears to
be one of the offending windows with a timestamp of 5598418. Working around...
Oct 15 18:16:29 vmshutenko gnome-shell[1690]: Window manager warning: last user time
(5600465) is greater than comparison timestamp (5600463). This most likely represe
nts a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WIN
DOW. Trying to work around...
Oct 15 18:16:29 vmshutenko gnome-shell[1690]: Window manager warning: W5 appears to
be one of the offending windows with a timestamp of 5600465. Working around...
Oct 15 18:18:43 vmshutenko systemd[1583]: vte-spawn-90bda244-4d64-4da9-a016-3721dffb
2113.scope: Consumed 13.400s CPU time.
Oct 15 18:18:45 vmshutenko systemd[1583]: Started VTE child process 4097 launched by
gnome-terminal-server process 2336.
Oct 15 18:18:50 vmshutenko systemd[1]: Starting Fingerprint Authentication Daemon...
Oct 15 18:18:50 vmshutenko systemd[1]: Started Fingerprint Authentication Daemon.
Oct 15 18:18:53 vmshutenko su[4124]: (to root) vmshutenko on pts/0
Oct 15 18:19:21 vmshutenko systemd[1]: fprintd.service: Deactivated successfully.
[root@vmshutenko html]#
```

Figure 17: Системный лог-файл.

Просмотр лог-файла audit.log



```
vmshutenko@vmshutenko:/var/www/html x mc [root@vmshutenko]:/var/log/audit x
audit.log [-M--] 0 L:[ 1+ 0 1/2862] *(0 /653128b) 0116 0x074 [*][X]
type=DAEMON_START msg=audit(1662938104.359:4539): op=start ver=3.0.7 format=enriched
type=SERVICE_START msg=audit(1662938104.417:5): pid=1 uid=0 auid=4294967295 ses=4294
type=CONFIG_CHANGE msg=audit(1662938104.780:6): op=set audit backlog_limit=8192 old=
type=SYSCALL msg=audit(1662938104.780:6): arch=c000003e syscall=44 success=yes exit=
type=PROCTITLE msg=audit(1662938104.780:6): proctitle=2F7362696E2F617564697463746C00
type=CONFIG_CHANGE msg=audit(1662938104.783:7): op=set audit_failure=1 old=1 auid=42
type=SYSCALL msg=audit(1662938104.783:7): arch=c000003e syscall=44 success=yes exit=
type=PROCTITLE msg=audit(1662938104.783:7): proctitle=2F7362696E2F617564697463746C00
type=CONFIG_CHANGE msg=audit(1662938104.785:8): op=set audit backlog_wait time=60000
type=SYSCALL msg=audit(1662938104.785:8): arch=c000003e syscall=44 success=yes exit=
type=PROCTITLE msg=audit(1662938104.785:8): proctitle=2F7362696E2F617564697463746C00
type=SERVICE_START msg=audit(1662938104.805:9): pid=1 uid=0 auid=4294967295 ses=4294
type=SYSTEM_BOOT msg=audit(1662938104.905:10): pid=728 uid=0 auid=4294967295 ses=429
type=SERVICE_START msg=audit(1662938104.941:11): pid=1 uid=0 auid=4294967295 ses=429
type=SERVICE_START msg=audit(1662938106.246:12): pid=1 uid=0 auid=4294967295 ses=429
type=SERVICE_START msg=audit(1662938106.298:13): pid=1 uid=0 auid=4294967295 ses=429
type=BPF msg=audit(1662938106.344:14): prog-id=28 op=LOAD
type=SERVICE_START msg=audit(1662938106.563:15): pid=1 uid=0 auid=4294967295 ses=429
type=BPF msg=audit(1662938106.617:16): prog-id=29 op=LOAD
type=SERVICE_START msg=audit(1662938106.730:17): pid=1 uid=0 auid=4294967295 ses=429
type=SERVICE_START msg=audit(1662938106.784:18): pid=1 uid=0 auid=4294967295 ses=429
type=BPF msg=audit(1662938107.533:19): prog-id=30 op=LOAD
type=BPF msg=audit(1662938107.561:20): prog-id=31 op=LOAD
1Помощь 2Сох-ть 3Злук 4Замена 5Копия 6Пер-ть 7Поиск 8Уда-ть 9МенюМС 10Выход
```

Figure 18: Лог-файл audit.log.

Добавление порта 81.

```
Oct 19 18:19:21 vmshutenko systemd[1]: tprintd.service: deactivated successfully.
[root@vmshutenko html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@vmshutenko html]# semanage port -l | grep http_port_t
bash: grep http_port_t: command not found...
^[[A[root@vmshutenko htm
[root@vmshutenko html]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@vmshutenko html]#
```

Figure 19: Добавление порта 81.

Удаление порта 81.

```
[root@vmshutenko html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vmshutenko html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@vmshutenko html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@vmshutenko html]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@vmshutenko html]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@vmshutenko html]# cd /var/www/html/
[root@vmshutenko html]# ls
[root@vmshutenko html]#
```

Figure 20: Возвращение контекста, удаление привязки к порту 81 и удаление файла test.html.

Итоги выполнения лабораторной работы

- Получили первое практическое знакомство с технологией SELinux1.
- Проверили работу SELinux на практике совместно с веб-сервером Apache.
- Создали файл test.html.