

# Лабораторная работа №6

## Мандатное разграничение прав в Linux

---

Ким М. А.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

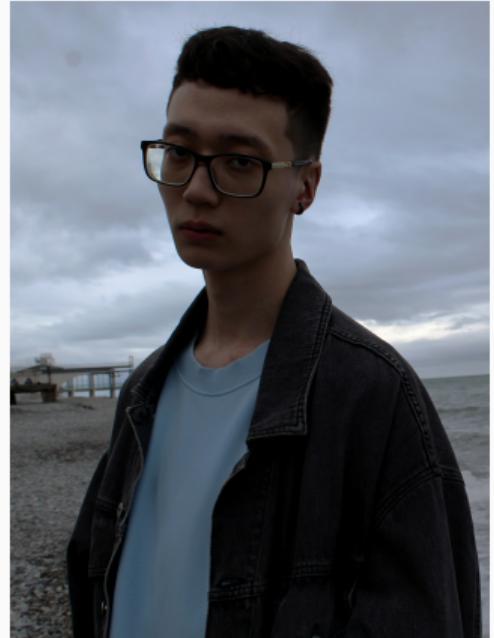
# Информация

---

# Докладчик

---

- Ким Михаил Алексеевич
- студент уч. группы НФИбд-01-20
- Российский университет дружбы народов
- 1032201664@pfur.ru
- <https://github.com/exmanka>



## **Вводная часть**

---

## Актуальность

---

- Необходимость навыков работы с различными ОС, git, Markdown.

## Объект и предмет исследования

---

- Операционная система Rocky Linux
- SELinux
- Apache
- Язык разметки Markdown

## Цели и задачи

---

- Развитие навыков администрирования ОС Linux. Получение первого практического знакомства с технологией принудительного контроля доступа SELinux. Проверка работы SELinux на практике совместно с веб-сервером Apache.

## **Процесс выполнения работы**

---

## Получение информации о работе SELinux. Установка и проверка Apache

```
[makim@makim ~]$ getenforce
Enforcing
[makim@makim ~]$ 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
[makim@makim ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
```

```
[root@localhost ~]# sudo systemctl install httpd
Last metadata expiration check: 0:05:07 ago on Sat 21 Oct 2023 07:55:36 PM HSK.
Package httpd-2.4.53-11.el9.3.5.sdb_64 is already installed.
Dependencies resolved.

Nothing to do.
Complete!
[root@localhost ~]# systemctl httpd status
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: off)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
```

# Получение информации о работе Apache

```
[makim@makim ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event               off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_ jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius                off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                   on
cdrecord_read_content          off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write              off
cobbler_can_network_connect    off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect   off
colorl_use_nfs                  off
condor_tcp_network_connect     off
conman_can_network              off
conman_use_nfs                  off
container_connect_any           off
container_manage_cgroup          off
container_use_cephfs            off
container_use_devices           off
container_use_encryptfs          off
cron_can_relabel                off
cron_system_cronjob_use_shares off
cron_userdomain_transition      on
cups_execmem                     off
cvs_read_shadow                 off
daemons_dontaudit_scheduling   on
daemons_dump_core               off
daemons_enable_cluster_mode     off
daemons_use_tcp_wrapper          off
daemons_use_tty                  off
```

```
[makim@makim ~]$ lsinfo
lsinfo: seinfo command not found...
Install package "selinux-console" to provide command 'seinfo'? [N/y] y

+ waiting in queue...
The following packages have to be installed:
selinux-console-4.4.1-1.el9.x86_64          Policy analysis command-line tools for SELinux
process with changes? [N/y] y

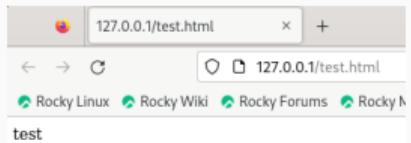
+ Waiting in queue...
+ Waiting for authentication...
+ Waiting in queue...
+ Downloading packages...
+ Preparing...
+ Testing changes...
+ Installing packages...
statistics for policy file: /sys/fs/selinux/policy
Policy version: 33 (MLS enabled)
Target Policy:
Handle unknown classes: allow
Classes: 135 Permissions: 457
Sensitivitylevels: 1 Categories: 3804
Types: 5100 Attributes: 258
Users: 8 Roles: 14
Booleans: 353 Cond. Expr.: 384
Allow: 65988 Neverallow: 0
Auditallow: 170 Demandallow: 8572
Type_trans: 265384 Type_change: 0
Initial SIDS: 27 Fa_Users: 15
Userfcons: 199 Portcons: 660
Netfcons: 0 Nodecon: 0

[makim@makim ~]$ ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

```
[makim@makim ~]$ ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

```
[makim@makim ~]$ ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

# Отображение HTML-файла. Изменение контекста файла. Просмотр логов



```
[makim@makim ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

```
[makim@makim ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
(sudo) password for makim:
[makim@makim ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[makim@makim ~]$ wget ls -Z /var/www/html/test.html
wget: invalid option -- 'Z'
Usage: wget [OPTION]... [URL]...
Try 'wget --help' for more options.
[makim@makim ~]$ wget http://127.0.0.1/test.html
--2023-10-21 20:22:35-- http://127.0.0.1/test.html
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2023-10-21 20:22:35 ERROR 403: Forbidden.
```

```
[makim@makim ~]$ curl -v http://127.0.0.1/test.html
*   Trying 127.0.0.1:80...
* TCP_NODELAY set
* Connected to 127.0.0.1 (127.0.0.1) port 80 (#0)
* Server certificate:
*   subject: CN=127.0.0.1
*   start date: Oct 21 2023 19:45:40 GMT
*   expire date: Oct 21 2024 19:45:40 GMT
*   issuer: /C=US/O=DigiCert Inc/CN=DigiCert Global Root CA
*   SSL certificate verify result: self signed certificate (1)
*   ciphers: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
*   compression: zdeflate
*   TLS handshake successful!
< HTTP/1.1 403 Forbidden
< Date: Mon, 21 Oct 2023 20:22:35 GMT
< Content-Type: text/html
< Content-Length: 14
< Connection: close
<
* Connection #0 to host 127.0.0.1 left intact
* Closing connection 0
2023-10-21 20:22:35 ERROR 403: Forbidden.
```

## Изменение прослушиваемого TCP-порта для Apache

This is the main Apache HTTP server configuration file. It contains the configuration for the server as well as several important directives for modules included with the server.

For more information about this file, see the [Apache Configuration](#) document.

See the [Apache Configuration](#) man page for more information on this file's parameters, and [httpd.conf\(5\)](#) for an log and configuring the httpd service.

If you are trying to have the webserver to serve without understanding what it is doing, then you are in for a surprise. If you are unsure about what you are doing, then you have been warned.

The `DocumentRoot` directive specifies the path to the directory where the various web pages are stored. The following example specifies the `/var/www/html` directory as the `DocumentRoot`. Note that the `DocumentRoot` directive can be specified at multiple levels. In this example, the `DocumentRoot` is specified at the top level, and then again inside the `<VirtualHost>` block. The value of `DocumentRoot` is relative to the current directory. For example, if the `DocumentRoot` were set to `/var/www/html/test`, then all `URI`s containing `/test` would be interpreted as `/var/www/html/test`.

**Important:** The use of the `DocumentRoot` directive under the `<VirtualHost>` block is not recommended.

If you are trying to serve files from a specific directory, then you must `DocumentRoot` or a `<VirtualHost>` block to specify a local `path` on the server. If you are trying to serve files from a remote location, then you must use the `Alias` directive. For authority except aliases, you will need to change an `AccessFileName` to `allowOverride All`.

**ServerName "VHOSTNAME"**

`listen` allows you to bind specific IP addresses and/or ports to the default, but also the `vhosts` directive.

`ChangeDir` is listed as a specific `IP address`, but note that it is not required to be a specific IP address. It can also be a port number or a `URI` to which the reverse proxy clients. See the `httpd-alias(5)` man page for more information.

**Listen 21,60,70,80**

**Status 81**

**Dynamic Shared Object (DSO) Handler**

You will be able to use the functionality of a module which was built as a DSO you can load/unload them. This is useful for security reasons, or if you want to add/directives contained in a dynamically loaded module. If you do not need to do this, then leave this out.

**LoadModule mod\_so.c**

**LoadModule mod\_index.c**

**If you wish to use it as a different user or group, you must run**

**httpd -k start**

File	Type	Description
httpd	DSO	For Web
mod_index	DSO	Apache Handler
mod_so	DSO	Apache Handler
httpd-fpm	DSO	Apache Handler

```
[makin@makin ~]$ semanage port -l | grep http_port_t
Error: SELinux policy is not managed or store cannot be accessed.
[makin@makin ~]$ sudo semanage port -l | grep http_port_t
http_port_t          tcp    80, 81, 443, 488, 8000, 8080, 8443, 9000
pegasus_http_port_t  tcp    5988
```

test

arrow keys to move up and down. Right to follow a link; Left to go back.  
Arrow keys to scroll down to move. Right to follow a link; Left to go back.  
Help Options Print Die Main screen Gnutt (-search {object})-History List

```
    if (is_prime(n)) {
        for (int i = 2; i < n; i++) {
            if (n % i == 0) {
                cout << "Not prime" << endl;
                return 0;
            }
        }
        cout << "Prime" << endl;
    }
    return 0;
}
```

# Обратное изменение прослушиваемого TCP-порта для Apache. Удаление созданных файлов

```
GNU nano 3.6.1                               /etc/httpd/conf/httpd.conf

This is the main Apache HTTP server configuration file. It contains the
configuration directives that give the server its instructions.
See http://httpd.apache.org/docs/2.4/ for detailed information.
In particular, see
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: http://httpd.apache.org/docs/2.4/. 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
configuration, error, and log files are kept.

Do not add a slash at the end of the directory path. If you point
ServerRoot at a non-local disk, be sure to specify a local disk on the
Mutex directive, if file-based mutexes are used. If you wish to share the
same ServerRoot for multiple httpd daemons, you will need to change at
least PidFile.

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 80

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
to be loaded here.

Example:
LoadModule foo_module modules/mod_foo.so

Include conf.modules.d/*.conf

If you wish httpd to run as a different user or group, you must run
httpd as root (privileges are still retained).
```

```
[makim@makim ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

```
[makim@makim ~]$ sudo nano /etc/httpd/conf/httpd.conf
[makim@makim ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: SELinux policy is not managed or store cannot be accessed.
[makim@makim ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[makim@makim ~]$ sudo semanage port -l | grep http_port_t
http_port_t          tcp    80, 81, 443, 488, 8008, 8089, 8443, 9008
pegasus_http_port_t  tcp    5988
[makim@makim ~]$ sudo semanage port -l | grep http_port_t
http_port_t          tcp    80, 81, 443, 488, 8008, 8089, 8443, 9008
pegasus_http_port_t  tcp    5988
[makim@makim ~]$ rm /var/www/html/test.html
rm: remove write-protected regular file '/var/www/html/test.html'? y
rm: cannot remove '/var/www/html/test.html': Permission denied
[makim@makim ~]$ sudo rm /var/www/html/test.html
[makim@makim ~]$ ll /var/www/html
total 8
```

## Результаты

---

# Результаты

---

- Выполнены все необходимые задания.

## Вывод

Развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работа SELinux на практике совместно с веб-сервером Apache.