

# Лабораторная работа №6

Основы информационной безопасности

---

Ищенко Ирина

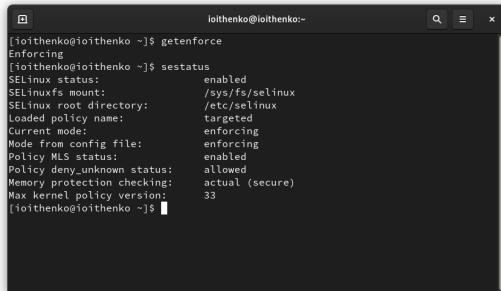
Российский университет дружбы народов, Москва, Россия

- Ищенко Ирина Олеговна
- НПИбд-02-22

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

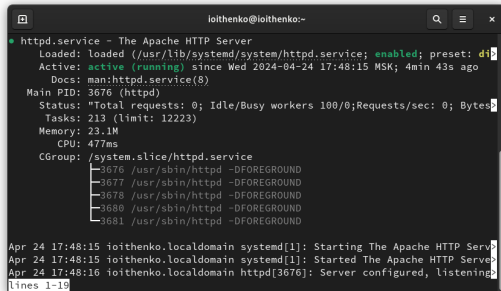
## Выполнение лабораторной работы

---

A terminal window with a dark background and light text. The window title is 'loithenko@loithenko:~'. It shows the output of two commands: 'getenforce' and 'sestatus'. The 'getenforce' command returns 'Enforcing'. The 'sestatus' command returns a detailed status report for SELinux, including its status, mount point, root directory, loaded policy name, current mode, mode from config file, policy MLS status, policy deny\_unknown status, memory protection checking, and max kernel policy version.

```
[loithenko@loithenko ~]$ getenforce
Enforcing
[loithenko@loithenko ~]$ 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
[loithenko@loithenko ~]$
```

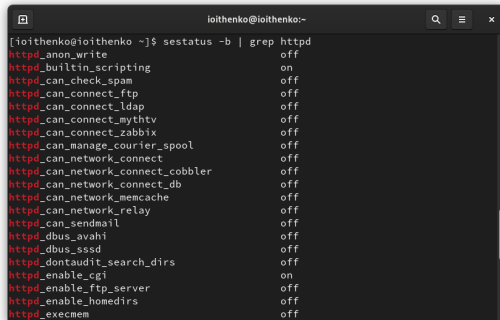
Рис. 1: Проверка статуса



```
ioithenko@ioithenko:~$ systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-04-24 17:48:15 MSK; 4min 43s ago
     Docs: man:httpd.service(8)
   Main PID: 3676 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
   Tasks: 213 (limit: 12223)
  Memory: 23.1M
    CPU: 477ms
   CGroup: /system.slice/httpd.service
           └─3676 /usr/sbin/httpd -DFOREGROUND
             └─3677 /usr/sbin/httpd -DFOREGROUND
               └─3678 /usr/sbin/httpd -DFOREGROUND
                 └─3680 /usr/sbin/httpd -DFOREGROUND
                   └─3681 /usr/sbin/httpd -DFOREGROUND

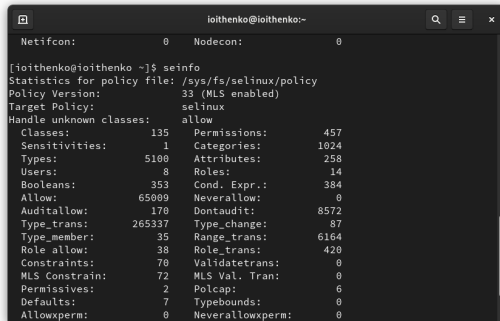
Apr 24 17:48:15 ioithenko.localdomain systemd[1]: Starting The Apache HTTP Server:
Apr 24 17:48:15 ioithenko.localdomain systemd[1]: Started The Apache HTTP Server:
Apr 24 17:48:16 ioithenko.localdomain httpd[3676]: Server configured, listening on
lines 1-19
```

Рис. 2: Проверка статуса



```
ioithenko@ioithenko:~  
[ioithenko@ioithenko ~]$ sestatus -b | grep httpd  
httpd_anon_write off  
httpd_builtin_scripting on  
httpd_can_check_spam off  
httpd_can_connect_ftp off  
httpd_can_connect_ldap off  
httpd_can_connect_mythtv off  
httpd_can_connect_zabbix off  
httpd_can_manage_courier_spool off  
httpd_can_network_connect off  
httpd_can_network_connect_cobbler off  
httpd_can_network_connect_db off  
httpd_can_network_memcache off  
httpd_can_network_relay off  
httpd_can_sendmail off  
httpd_dbus_avahi off  
httpd_dbus_sssd off  
httpd_dontaudit_search_dirs off  
httpd_enable_cgi on  
httpd_enable_ftp_server off  
httpd_enable_homedirs off  
httpd_execmem off
```

Рис. 3: Переключатели

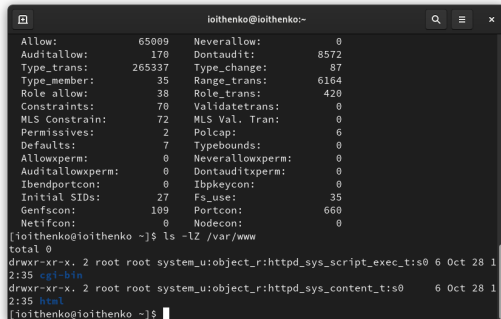


```
ioithenko@ioithenko:~  
Netifcon: 0 Nodecon: 0  
[ioithenko@ioithenko ~]$ seinfo  
Statistics for policy file: /sys/fs/selinux/policy  
Policy Version: 33 (MLS enabled)  
Target Policy: selinux  
Handle unknown classes: allow  
Classes: 135 Permissions: 457  
Sensitivities: 1 Categories: 1024  
Types: 5100 Attributes: 258  
Users: 8 Roles: 14  
Booleans: 353 Cond. Expr.: 384  
Allow: 65009 Neverallow: 0  
Auditallow: 170 Dontaudit: 8572  
Type_trans: 265337 Type_change: 87  
Type_member: 35 Range_trans: 6164  
Role allow: 38 Role_trans: 420  
Constraints: 70 Validatetrans: 0  
MLS Constrain: 72 MLS Val. Tran: 0  
Permissives: 2 Polcap: 6  
Defaults: 7 Typebounds: 0  
Allowxperm: 0 Neverallowxperm: 0
```

Рис. 4: Статистика по политике



# Типы файлов и поддиректории

A terminal window titled 'ioithenko@ioithenko:~' with search, menu, and close buttons. It displays a list of file types and their counts, followed by a command to list files in /var/www with long format and long listing options. The output shows two directories: 'cgi-bin' and 'html', both with permissions 'drwxr-xr-x', owned by 'root', and containing files from '6 Oct 28 12:35'.

```
ioithenko@ioithenko:~  
Allow: 65009 Neverallow: 0  
Auditallow: 170 Dontaudit: 8572  
Type_trans: 265337 Type_change: 87  
Type_member: 35 Range_trans: 6164  
Role_allow: 38 Role_trans: 420  
Constraints: 70 Validatetrans: 0  
MLS Constrain: 72 MLS Val. Tran: 0  
Permissives: 2 Polcap: 6  
Defaults: 7 Typebounds: 0  
Allowxperm: 0 Neverallowxperm: 0  
Auditallowxperm: 0 Dontauditxperm: 0  
Ibendportcon: 0 Ibpkeycon: 0  
Initial SIDs: 27 Fs_use: 35  
Genfscon: 109 Portcon: 660  
Netifcon: 0 Nodecon: 0  
[ioithenko@ioithenko ~]$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12:35 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12:35 html  
[ioithenko@ioithenko ~]$
```

Рис. 5: Типы файлов и поддиректории

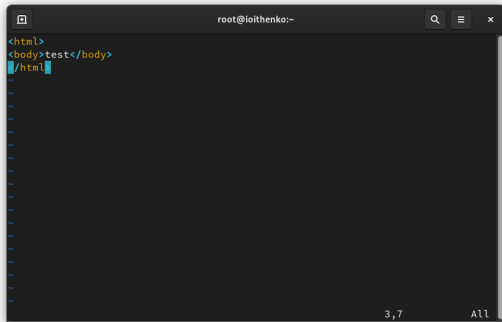
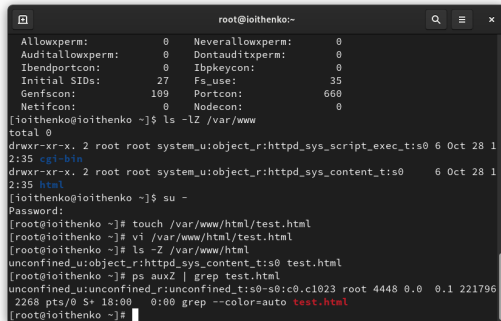


Рис. 6: Файл



```
root@ioithenko:~  
Allowxperm:      0   Neverallowxperm:      0  
Auditallowxperm:  0   Dontauditxperm:      0  
Ibendportcon:    0   Ibpkeycon:            0  
Initial SIDs:     27   Fs_use:               35  
Genfscon:         109   Portcon:              660  
Netifcon:         0   Nodecon:              0  
[ioithenko@ioithenko ~]$ ls -lZ /var/www  
total 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 1  
2:35 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 1  
2:35 html  
[ioithenko@ioithenko ~]$ su -  
Password:  
[root@ioithenko ~]# touch /var/www/html/test.html  
[root@ioithenko ~]# vi /var/www/html/test.html  
[root@ioithenko ~]# ls -lZ /var/www/html  
unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@ioithenko ~]# ps auxZ | grep test.html  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4448 0.0 0.1 221796  
2268 pts/0 S+ 18:00 0:00 grep --color=auto test.html  
[root@ioithenko ~]#
```

Рис. 7: Контекст

# Проверка отображения файла

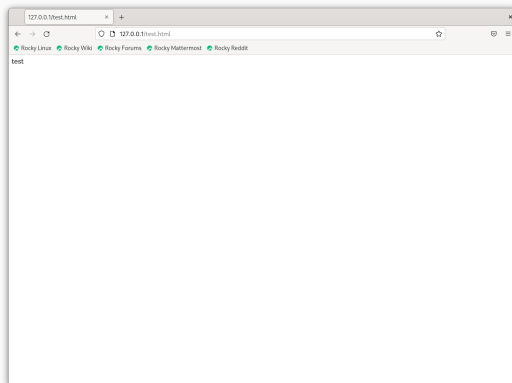
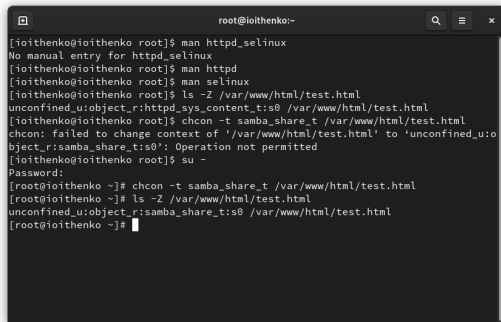


Рис. 8: Проверка отображения файла

A terminal window titled 'root@ioithenko:~' with search, menu, and close icons in the title bar. The terminal shows a series of commands and their outputs related to SELinux context management. The user 'ioithenko' is initially in the 'root' group. They run 'man httpd\_selinux' (no manual entry), 'man httpd', and 'man selinux'. Then they run 'ls -Z /var/www/html/test.html' showing context 'unconfined\_u:object\_r:httpd\_sys\_content\_t:s0'. Next, they run 'chcon -t samba\_share\_t /var/www/html/test.html', which fails with the message 'chcon: failed to change context of '/var/www/html/test.html' to 'unconfined\_u:object\_r:samba\_share\_t:s0': Operation not permitted'. Finally, they run 'su -' to become root. As root, they run 'chcon -t samba\_share\_t /var/www/html/test.html' successfully, and then 'ls -Z /var/www/html/test.html' again, showing the updated context 'unconfined\_u:object\_r:samba\_share\_t:s0'.

```
root@ioithenko:~  
[ioithenko@ioithenko root]$ man httpd_selinux  
No manual entry for httpd_selinux  
[ioithenko@ioithenko root]$ man httpd  
[ioithenko@ioithenko root]$ man selinux  
[ioithenko@ioithenko root]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[ioithenko@ioithenko root]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted  
[ioithenko@ioithenko root]$ su -  
Password:  
[root@ioithenko ~]# chcon -t samba_share_t /var/www/html/test.html  
[root@ioithenko ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@ioithenko ~]#
```

Рис. 9: Изменение контекста

# Проверка отображения файла

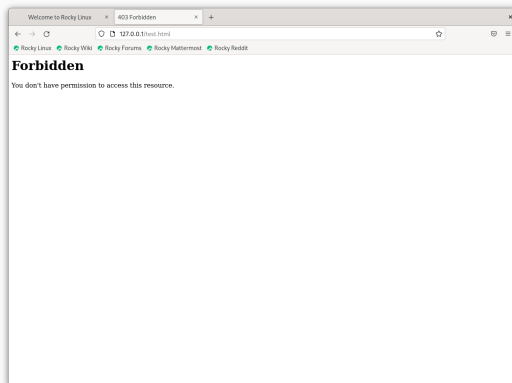
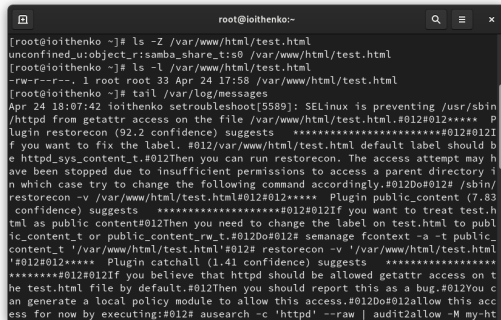
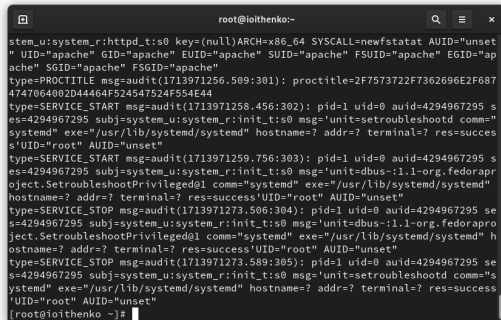


Рис. 10: Проверка отображения файла



```
root@ioithenko:~  
[root@ioithenko ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@ioithenko ~]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 Apr 24 17:58 /var/www/html/test.html  
[root@ioithenko ~]# tail /var/log/messages  
Apr 24 18:07:42 ioithenko setroubleshoot[5589]: SELinux is preventing /usr/sbin  
/httpd from getattr access on the file /var/www/html/test.html.#012#012***** P  
lugin restorecon (92.2 confidence) suggests *****#012#012I  
f you want to fix the label. #012/var/www/html/test.html default label should b  
e httpd_sys_content_t.#012Then you can run restorecon. The access attempt may h  
ave been stopped due to insufficient permissions to access a parent directory i  
n which case try to change the following command accordingly.#012Do#012# /sbin/  
restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83  
confidence) suggests *****#012#012If you want to treat test.h  
tml as public content#012Then you need to change the label on test.html to publ  
ic_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_  
content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html  
'#012#012***** Plugin catchall (1.41 confidence) suggests *****  
*****#012#012If you believe that httpd should be allowed getattr access on t  
he test.html file by default.#012Then you should report this as a bug.#012You c  
an generate a local policy module to allow this access.#012Do#012allow this acc  
ess for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-ht
```

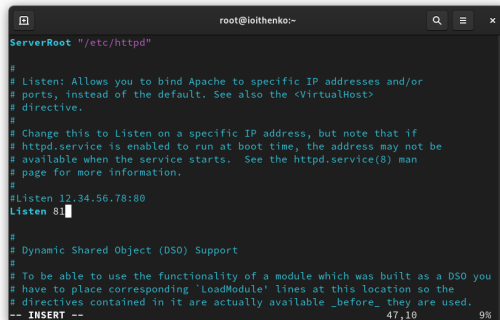
Рис. 11: Лог-файл



```
root@ioithenko:~  
stem_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset"  
" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="ap  
ache" SGID="apache" FSGID="apache"  
type=PROCTITLE msg=audit(1713971256.509:301): proctitle=2F7573722F7362696E2F687  
4747064002D44464F524547524F554E44  
type=SERVICE_START msg=audit(1713971258.456:302): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="s  
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=succes  
s'UID="root" AUID="unset"  
type=SERVICE_START msg=audit(1713971259.756:303): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapr  
oject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd"  
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.506:304): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapro  
ject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd" h  
ostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.589:305): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="s  
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success  
'UID="root" AUID="unset"  
[root@ioithenko ~]#
```

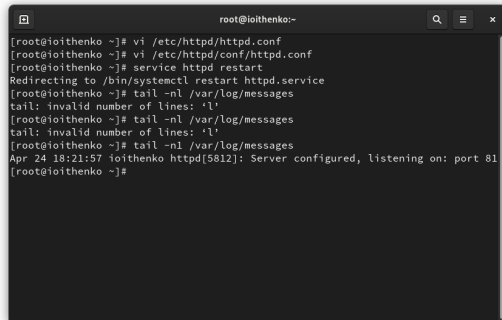
Рис. 12: /var/log/audit/audit.log





```
root@ioithenko:~  
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.  
-- INSERT --
```

Рис. 13: Замена порта



```
root@ioithenko:~  
[root@ioithenko ~]# vi /etc/httpd/httpd.conf  
[root@ioithenko ~]# vi /etc/httpd/conf/httpd.conf  
[root@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# tail -nl /var/log/messages  
tail: invalid number of lines: 'l'  
[root@ioithenko ~]# tail -n\ /var/log/messages  
tail: invalid number of lines: 'l'  
[root@ioithenko ~]# tail -n1 /var/log/messages  
Apr 24 18:21:57 ioithenko httpd[5812]: Server configured, listening on: port 81  
[root@ioithenko ~]#
```

Рис. 14: Лог-файл

```
root@ubuntu:~# cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: No such file or directory
root@ubuntu:~# cat /var/log/httpd/error_log
Wed Apr 24 17:48:15.720000 2024: [error] [pid 3678:tid 3678] MPM: pool
is enabled, httpd running as a systemd system, _httpd.pid
Wed Apr 24 17:48:15.822100 2024: [error:module] [pid 3678:tid 3678] core:1232
noEXEC module: module loaded: /usr/lib64/libc.so.6
Wed Apr 24 17:48:15.889700 2024: [warned:core:module] [pid 3678:tid 367
8] core:1232 no module from mod:core:module
Wed Apr 24 17:48:16.832410 2024: [warn:core:module] [pid 3678:tid 3678] AM0043
B: Apache/2.4.37 (Ubuntu) configured -- resuming normal operations
Wed Apr 24 17:48:16.832410 2024: [error:core] [pid 3678:tid 3678] AM00904: Co
re:module: module loaded: /usr/lib64/libc.so.6
Wed Apr 24 18:05:56.557400 2024: [error:core] [pid 3681:tid 3681] (12)Permission
denied: [client 127.0.0.1:41060] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:07:36.531445 2024: [error:core] [pid 3681:tid 3681] (11)Permission
denied: [client 127.0.0.1:50910] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:21:10.122000 2024: [warn:module] [pid 3678:tid 3678] AM0043
```

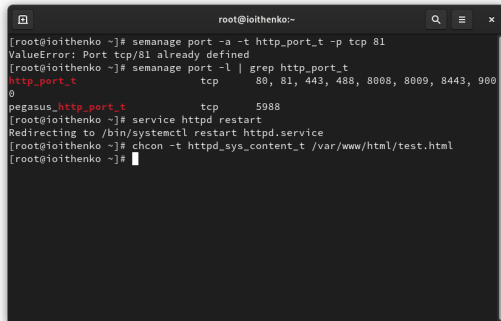
Рис. 15: /var/log/httpd/error\_log

```
root@ubuntu:~# cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: No such file or directory
root@ubuntu:~# cat /var/log/httpd/access_log
Wed Apr 24 18:21:10.122000 2024: [warn:module] [pid 3678:tid 3678] AM0043: Co
re:module: module loaded: /usr/lib64/libc.so.6
Wed Apr 24 18:05:56.557400 2024: [error:core] [pid 3681:tid 3681] (12)Permission
denied: [client 127.0.0.1:41060] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:07:36.531445 2024: [error:core] [pid 3681:tid 3681] (11)Permission
denied: [client 127.0.0.1:50910] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:21:10.122000 2024: [warn:module] [pid 3678:tid 3678] AM0043
```

Рис. 16: /var/log/httpd/access\_log

```
root@ubuntu:~# cat /var/log/audit/audit.log
cat: /var/log/audit/audit.log: No such file or directory
root@ubuntu:~# cat /var/log/audit/audit.log
Wed Apr 24 18:21:10.122000 2024: [warn:module] [pid 3678:tid 3678] AM0043: Co
re:module: module loaded: /usr/lib64/libc.so.6
Wed Apr 24 18:05:56.557400 2024: [error:core] [pid 3681:tid 3681] (12)Permission
denied: [client 127.0.0.1:41060] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:07:36.531445 2024: [error:core] [pid 3681:tid 3681] (11)Permission
denied: [client 127.0.0.1:50910] AH00015: access to /test.html denied (file
system path: /var/www/html/test.html) because search permissions are missing on
a component of the path
Wed Apr 24 18:21:10.122000 2024: [warn:module] [pid 3678:tid 3678] AM0043
```

Рис. 17: /var/log/audit/audit.log



```
root@ioithenko:~  
[root@ioithenko ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ioithenko ~]# 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@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ioithenko ~]#
```

Рис. 18: Контекст

# Проверка отображения файла

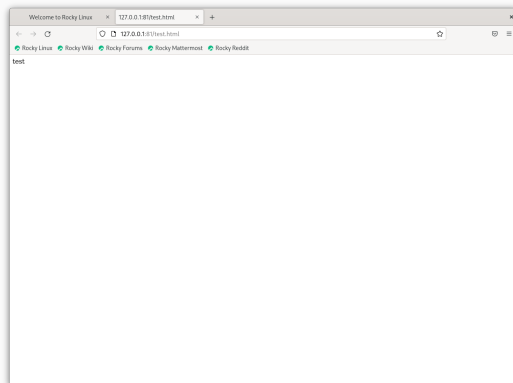
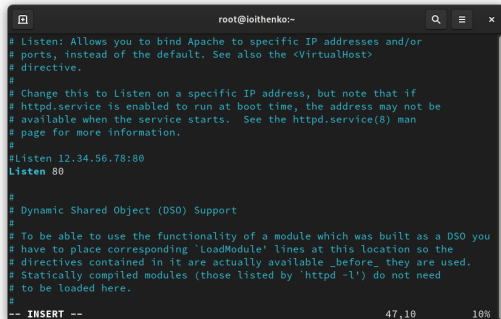


Рис. 19: Проверка отображения файла

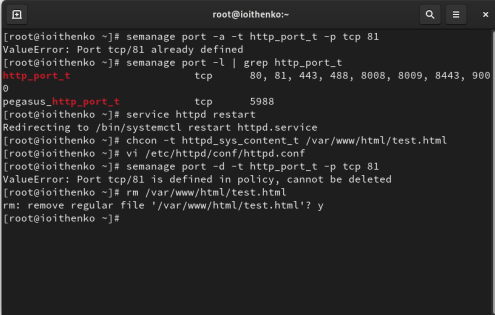
# Возвращение исходной конфигурации



```
root@ioithenko:~  
# 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.  
#  
-- INSERT --  
47,10 10%
```

Рис. 20: Возвращение исходной конфигурации

## Удаление привязки к порту и файла



```
root@ioithenko:~  
[root@ioithenko ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ioithenko ~]# 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@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ioithenko ~]# vi /etc/httpd/conf/httpd.conf  
[root@ioithenko ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted  
[root@ioithenko ~]# rm /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'? y  
[root@ioithenko ~]#
```

Рис. 21: Удаление привязки к порту и файла

В ходе лабораторной работы я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.