Защита лабораторной работы № 6. Мандатное разграничение прав в Linux

Смирнова Мария Александровна

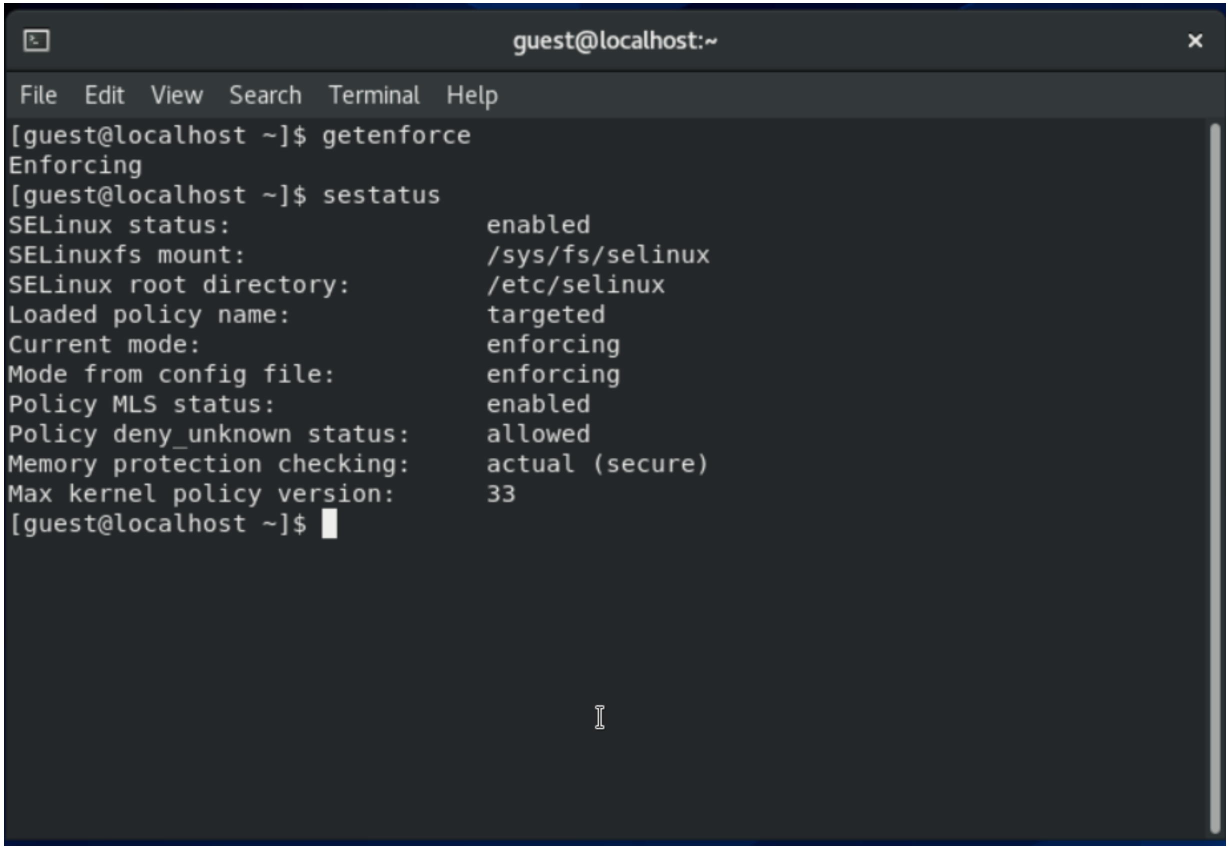
ЦЕЛЬ РАБОТЫ

Цель работы

Развитие навыков администрирования ОС Linux. Практическое освоение технологии SELinux. Проверка работы SELinux совместно с веб-сервером Apache.

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

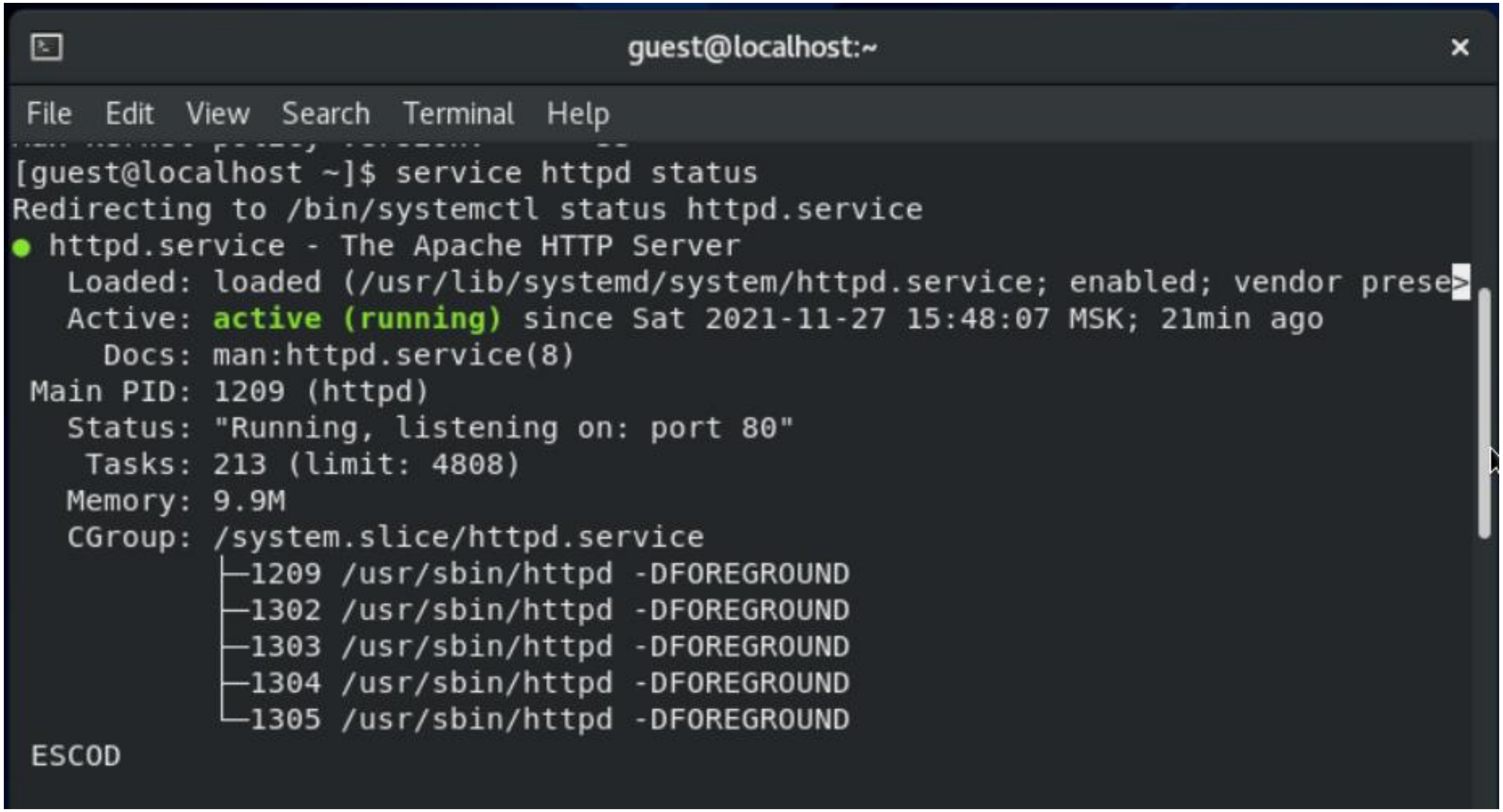
Выполнение лабораторной работы



```
[guest@localhost ~]$ getenforce
Enforcing
[guest@localhost ~]$ 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
[guest@localhost ~]$ 
```

Проверка SELinux

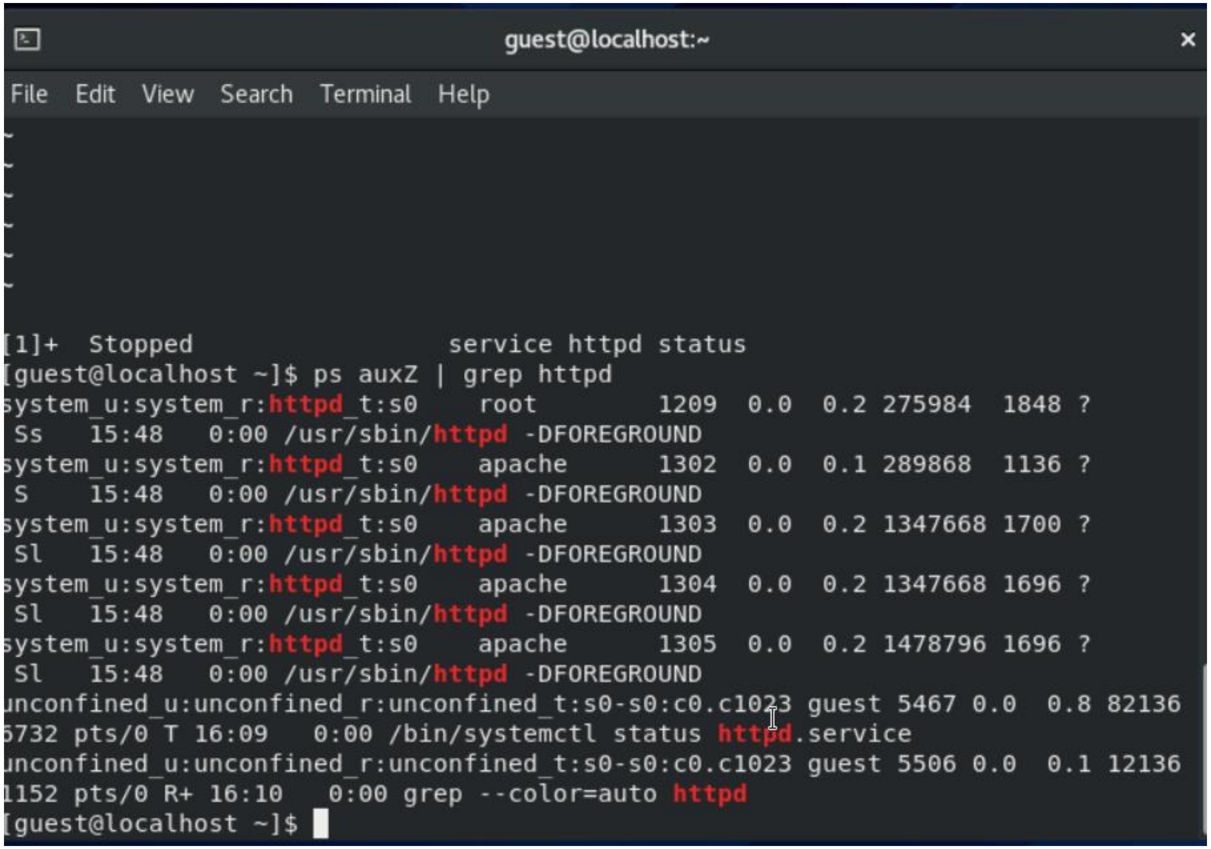
Выполнение лабораторной работы



```
[guest@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese>
   Active: active (running) since Sat 2021-11-27 15:48:07 MSK; 21min ago
     Docs: man:httpd.service(8)
 Main PID: 1209 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 4808)
   Memory: 9.9M
   CGroup: /system.slice/httpd.service
           ├─1209 /usr/sbin/httpd -DFOREGROUND
           ├─1302 /usr/sbin/httpd -DFOREGROUND
           ├─1303 /usr/sbin/httpd -DFOREGROUND
           ├─1304 /usr/sbin/httpd -DFOREGROUND
           └─1305 /usr/sbin/httpd -DFOREGROUND
 ESCOD
```

Httpd status

Выполнение лабораторной работы

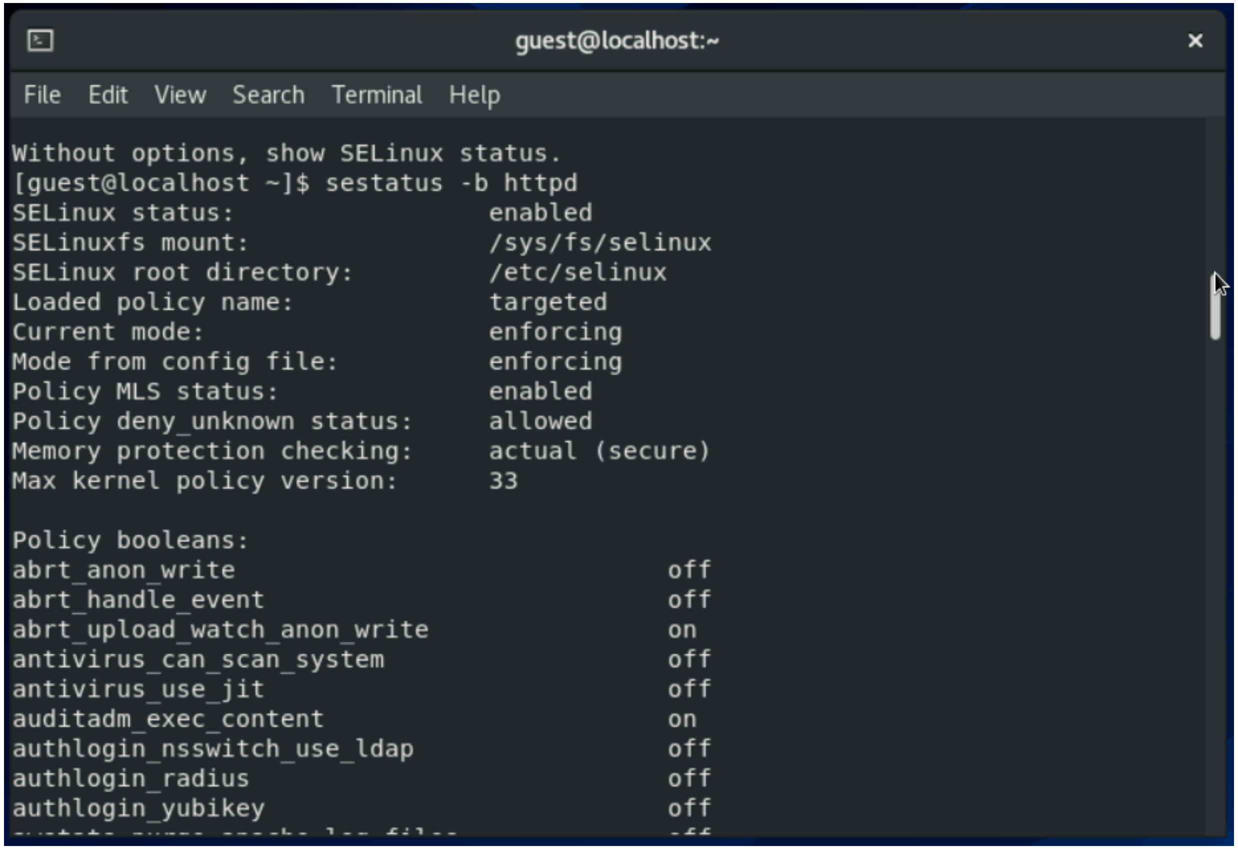


```
~
~
~
~
~
~

[1]+  Stopped                  service httpd status
[guest@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       1209  0.0  0.2 275984  1848 ?
 Ss   15:48   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     1302  0.0  0.1 289868  1136 ?
 S    15:48   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     1303  0.0  0.2 1347668 1700 ?
 Sl   15:48   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     1304  0.0  0.2 1347668 1696 ?
 Sl   15:48   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     1305  0.0  0.2 1478796 1696 ?
 Sl   15:48   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 guest 5467 0.0  0.8 82136
5732 pts/0 T 16:09   0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 guest 5506 0.0  0.1 12136
1152 pts/0 R+ 16:10   0:00 grep --color=auto httpd
[guest@localhost ~]$ 
```

Контекст безопасности Apache

Выполнение лабораторной работы

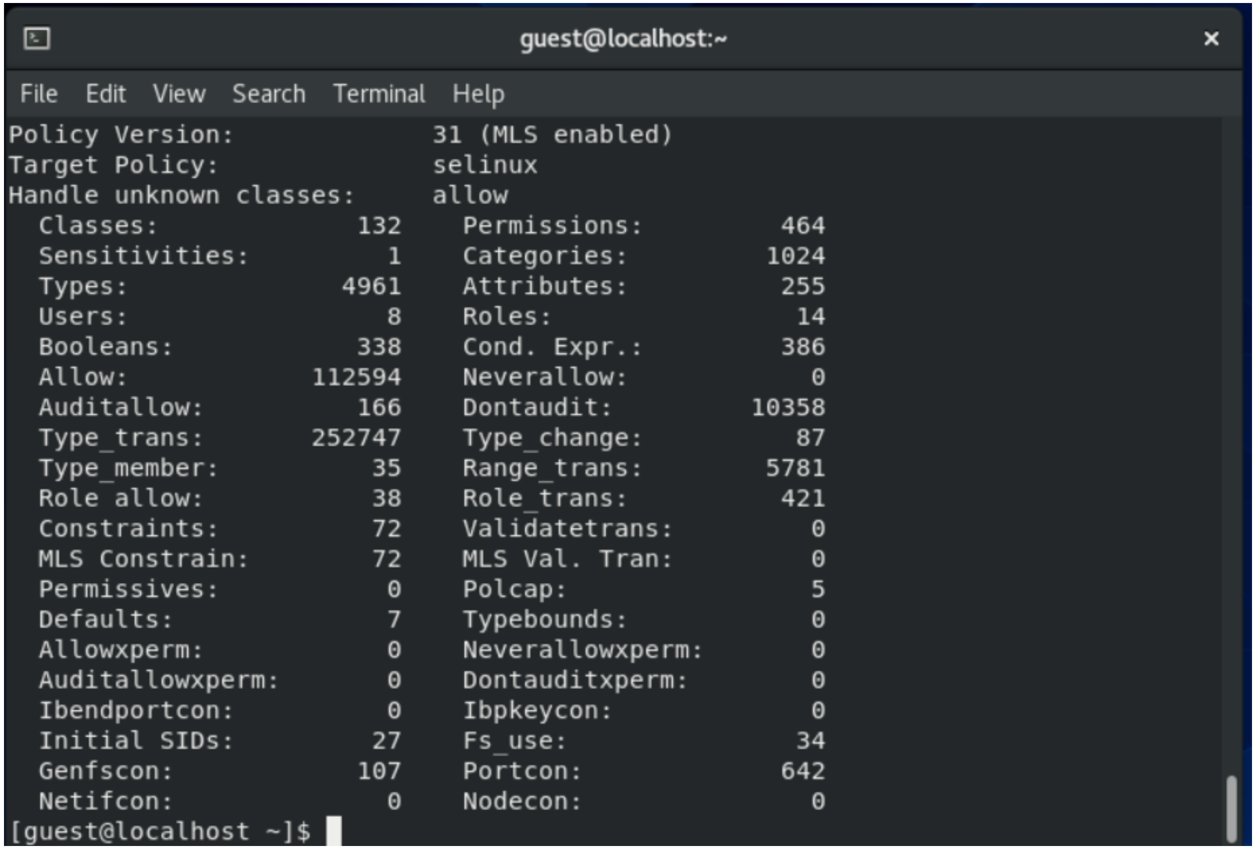


```
Without options, show SELinux status.
[guest@localhost ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode 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
```

Переключатели

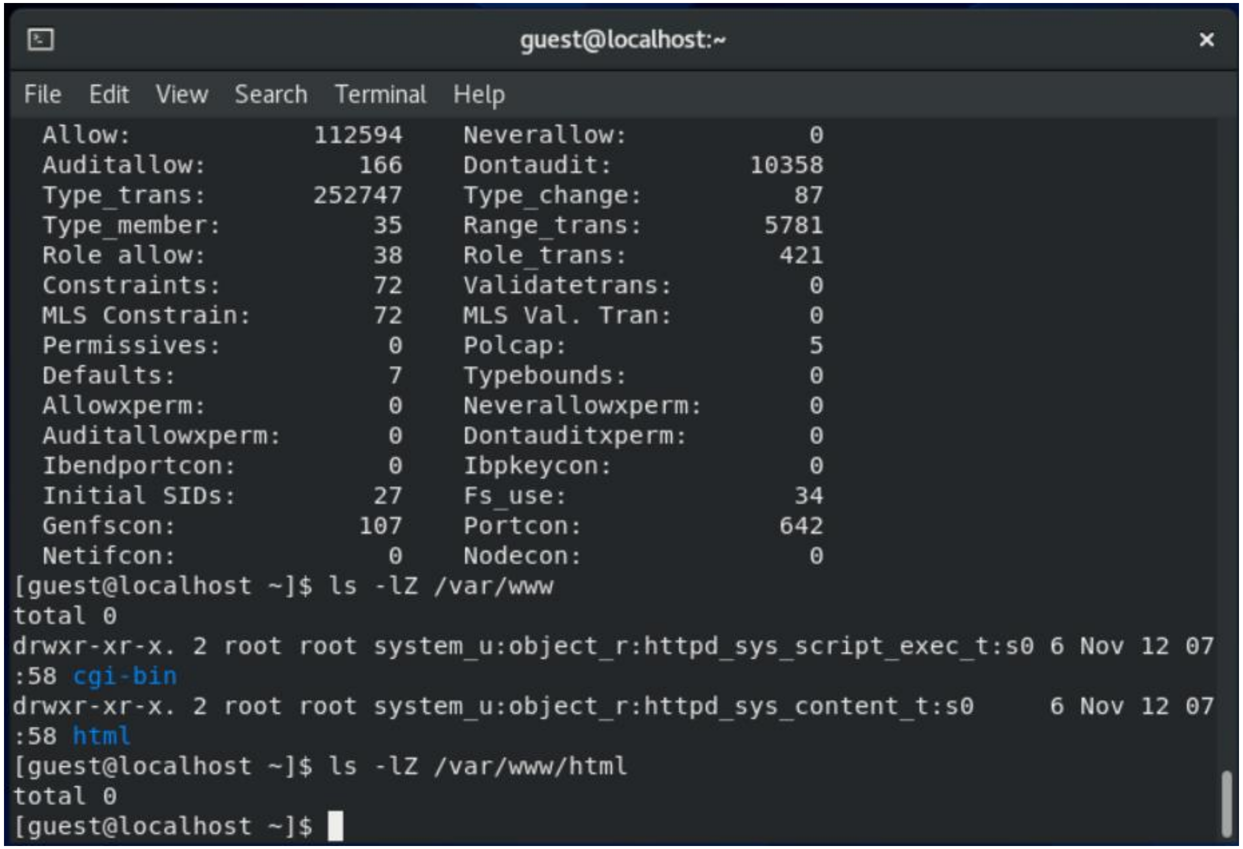
Выполнение лабораторной работы



```
Policy Version:              31 (MLS enabled)
Target Policy:               selinux
Handle unknown classes:      allow
  Classes:            132    Permissions:        464
  Sensitivities:        1    Categories:        1024
  Types:             4961    Attributes:         255
  Users:                8    Roles:               14
  Booleans:           338    Cond. Expr.:        386
  Allow:           112594    Neverallow:           0
  Auditallow:         166    Dontaudit:        10358
  Type_trans:      252747    Type_change:         87
  Type_member:         35    Range_trans:       5781
  Role allow:          38    Role_trans:         421
  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:              34
  Genfscon:           107    Portcon:            642
  Netifcon:             0    Nodecon:              0
[guest@localhost ~]$ 
```

Seinfo

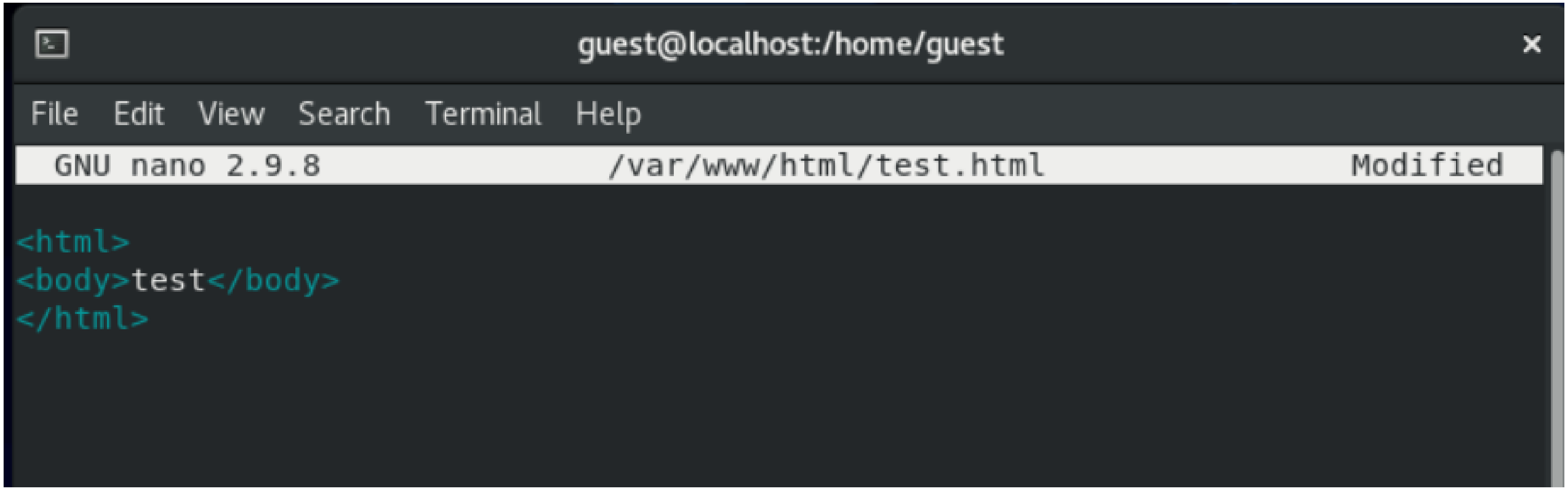
Выполнение лабораторной работы



```
  Allow:            112594    Neverallow:            0
  Auditallow:          166    Dontaudit:         10358
  Type_trans:       252747    Type_change:          87
  Type_member:          35    Range_trans:        5781
  Role allow:           38    Role_trans:          421
  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:               34
  Genfscon:            107    Portcon:             642
  Netifcon:              0    Nodecon:               0
[guest@localhost ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Nov 12 07
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 Nov 12 07
:58 html
[guest@localhost ~]$ ls -lZ /var/www/html
total 0
[guest@localhost ~]$ 
```

Директория /var/www/html

Выполнение лабораторной работы

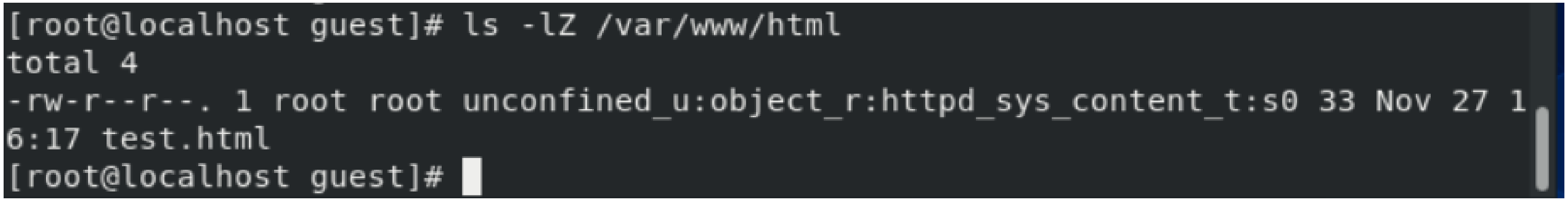

guest@localhost:/home/guest
File Edit View Search Terminal Help

```
  GNU nano 2.9.8             /var/www/html/test.html              Modified

<html>
<body>test</body>
</html>
```

test.html

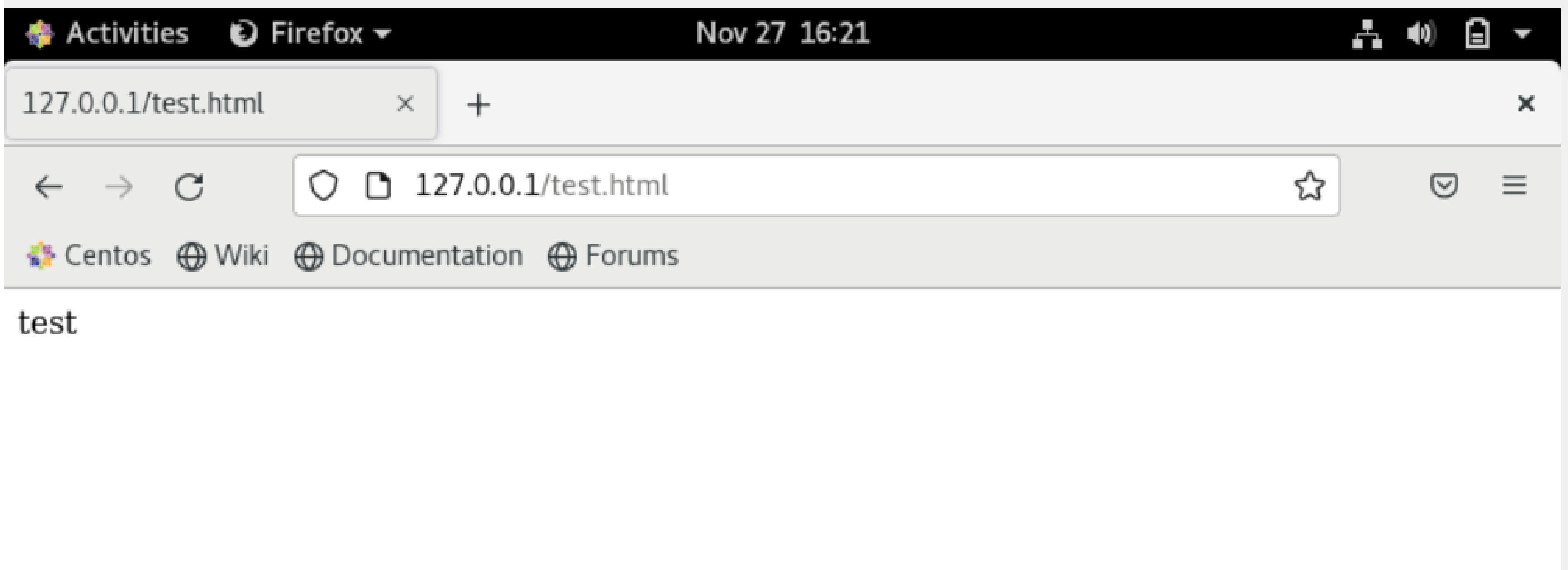
Выполнение лабораторной работы



```
[root@localhost guest]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Nov 27 1
6:17 test.html
[root@localhost guest]# 
```

Контекст test.html

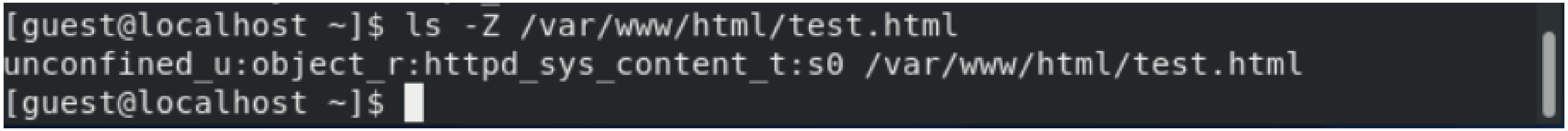
Выполнение лабораторной работы



test

http://127.0.0.1/test.html

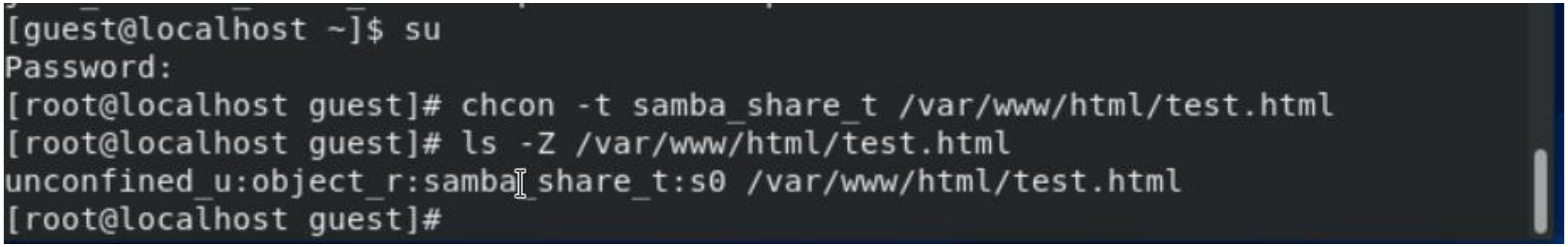
Выполнение лабораторной работы



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

Контексты файлов httpd

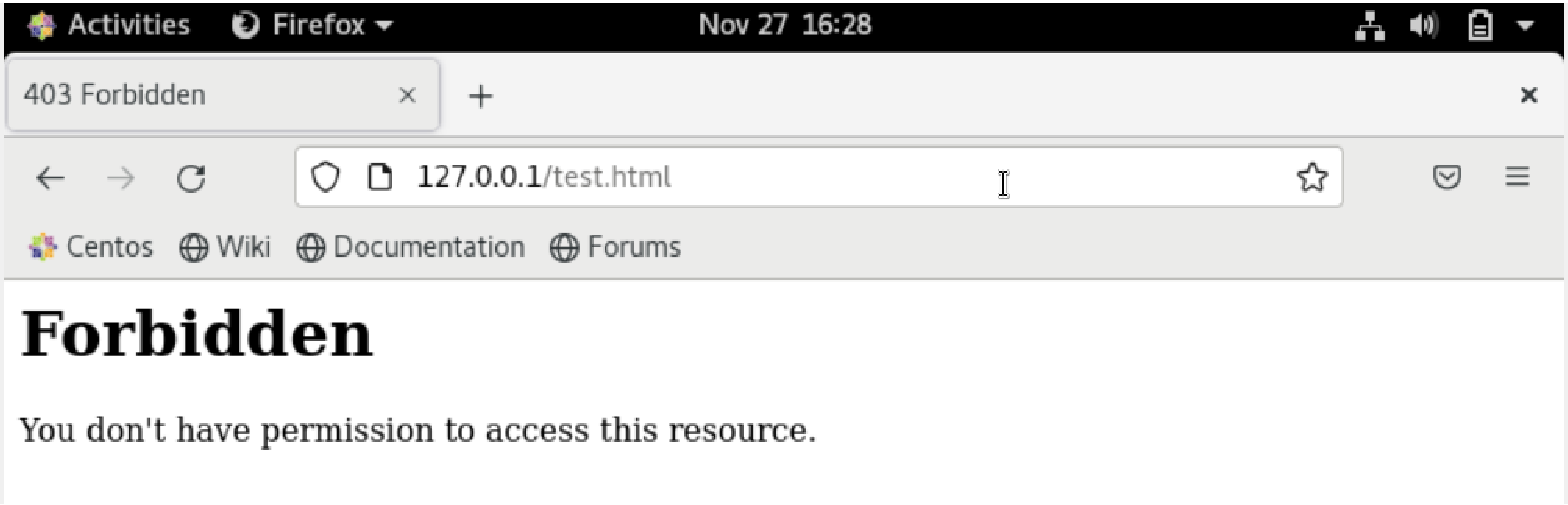
Выполнение лабораторной работы



```
[guest@localhost ~]$ su
Password:
[root@localhost guest]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost guest]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost guest]#
```

Изменение контекста test

Выполнение лабораторной работы

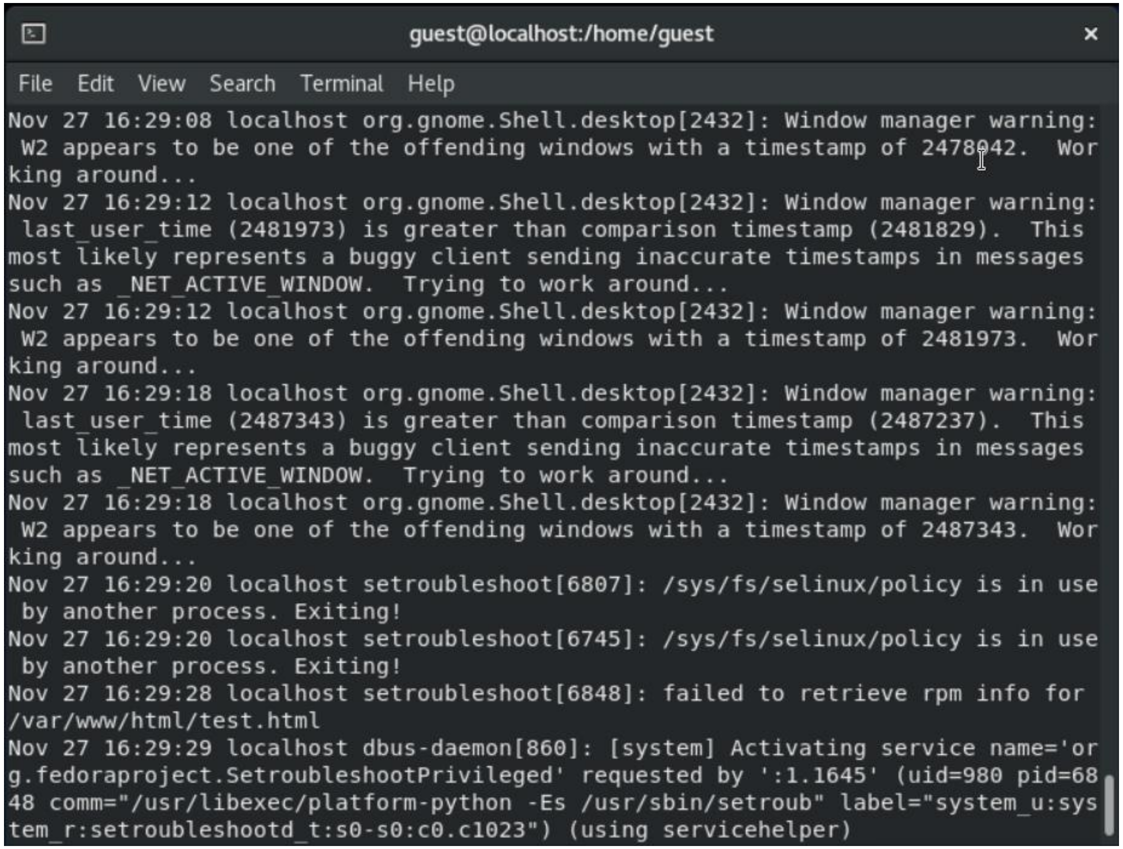


Forbidden

You don't have permission to access this resource.

Сообщение об ошибке

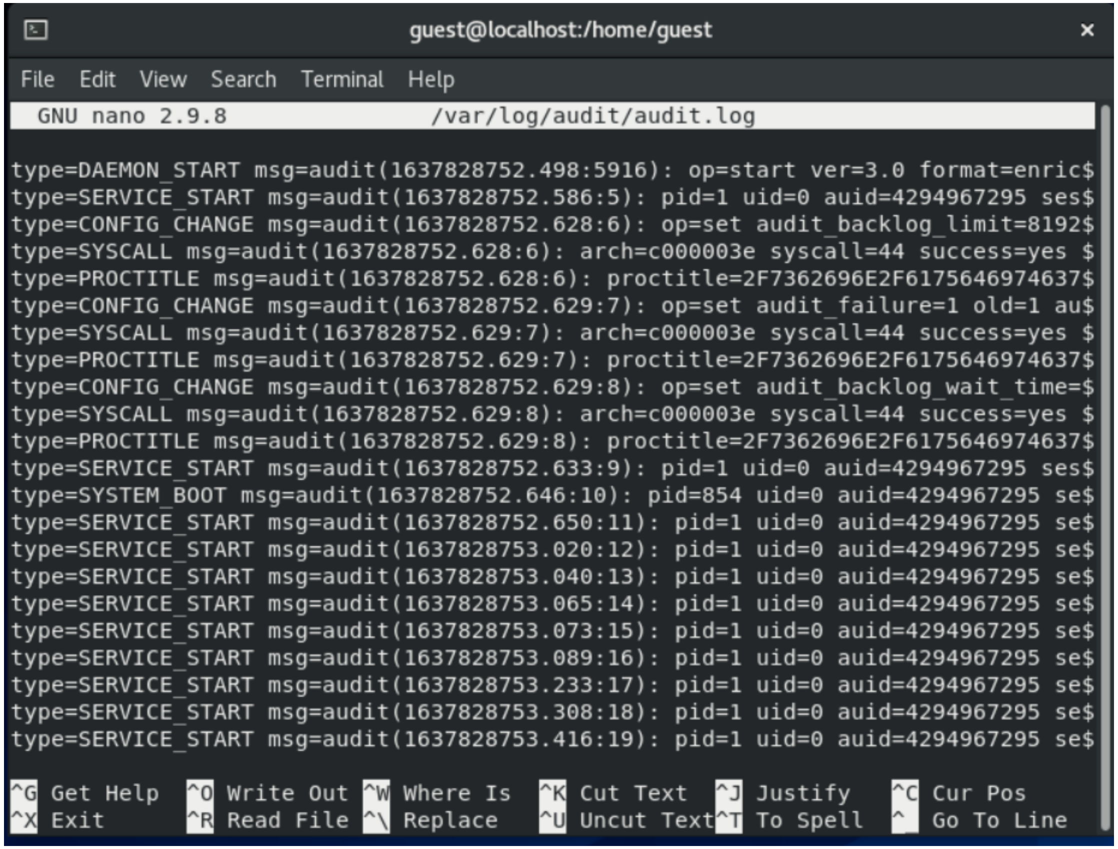
Выполнение лабораторной работы


guest@localhost:/home/guest
File Edit View Search Terminal Help

```
Nov 27 16:29:08 localhost org.gnome.Shell.desktop[2432]: Window manager warning:
 W2 appears to be one of the offending windows with a timestamp of 2478042.  Wor
king around...
Nov 27 16:29:12 localhost org.gnome.Shell.desktop[2432]: Window manager warning:
 last_user_time (2481973) is greater than comparison timestamp (2481829).  This
most likely represents a buggy client sending inaccurate timestamps in messages
such as _NET_ACTIVE_WINDOW.  Trying to work around...
Nov 27 16:29:12 localhost org.gnome.Shell.desktop[2432]: Window manager warning:
 W2 appears to be one of the offending windows with a timestamp of 2481973.  Wor
king around...
Nov 27 16:29:18 localhost org.gnome.Shell.desktop[2432]: Window manager warning:
 last_user_time (2487343) is greater than comparison timestamp (2487237).  This
most likely represents a buggy client sending inaccurate timestamps in messages
such as _NET_ACTIVE_WINDOW.  Trying to work around...
Nov 27 16:29:18 localhost org.gnome.Shell.desktop[2432]: Window manager warning:
 W2 appears to be one of the offending windows with a timestamp of 2487343.  Wor
king around...
Nov 27 16:29:20 localhost setroubleshoot[6807]: /sys/fs/selinux/policy is in use
 by another process. Exiting!
Nov 27 16:29:20 localhost setroubleshoot[6745]: /sys/fs/selinux/policy is in use
 by another process. Exiting!
Nov 27 16:29:28 localhost setroubleshoot[6848]: failed to retrieve rpm info for
/var/www/html/test.html
Nov 27 16:29:29 localhost dbus-daemon[860]: [system] Activating service name='or
g.fedoraproject.SetroubleshootPrivileged' requested by ':1.1645' (uid=980 pid=68
48 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:sys
tem_r:setroubleshootd_t:s0-s0:c0.c1023") (using servicehelper)
```

log-файл

Выполнение лабораторной работы


guest@localhost:/home/guest
File Edit View Search Terminal Help

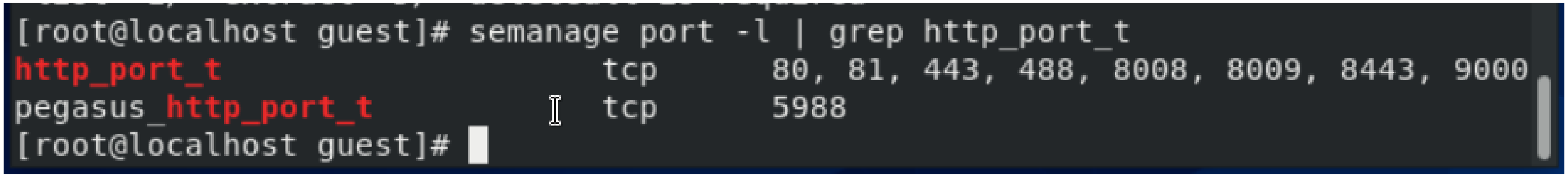
```
  GNU nano 2.9.8                 /var/log/audit/audit.log

type=DAEMON_START msg=audit(1637828752.498:5916): op=start ver=3.0 format=enric$
type=SERVICE_START msg=audit(1637828752.586:5): pid=1 uid=0 auid=4294967295 ses$
type=CONFIG_CHANGE msg=audit(1637828752.628:6): op=set audit_backlog_limit=8192$
type=SYSCALL msg=audit(1637828752.628:6): arch=c000003e syscall=44 success=yes $
type=PROCTITLE msg=audit(1637828752.628:6): proctitle=2F7362696E2F6175646974637$
type=CONFIG_CHANGE msg=audit(1637828752.629:7): op=set audit_failure=1 old=1 au$
type=SYSCALL msg=audit(1637828752.629:7): arch=c000003e syscall=44 success=yes $
type=PROCTITLE msg=audit(1637828752.629:7): proctitle=2F7362696E2F6175646974637$
type=CONFIG_CHANGE msg=audit(1637828752.629:8): op=set audit_backlog_wait_time=$
type=SYSCALL msg=audit(1637828752.629:8): arch=c000003e syscall=44 success=yes $
type=PROCTITLE msg=audit(1637828752.629:8): proctitle=2F7362696E2F6175646974637$
type=SERVICE_START msg=audit(1637828752.633:9): pid=1 uid=0 auid=4294967295 ses$
type=SYSTEM_BOOT msg=audit(1637828752.646:10): pid=854 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828752.650:11): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.020:12): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.040:13): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.065:14): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.073:15): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.089:16): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.233:17): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.308:18): pid=1 uid=0 auid=4294967295 se$
type=SERVICE_START msg=audit(1637828753.416:19): pid=1 uid=0 auid=4294967295 se$

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

audit.log

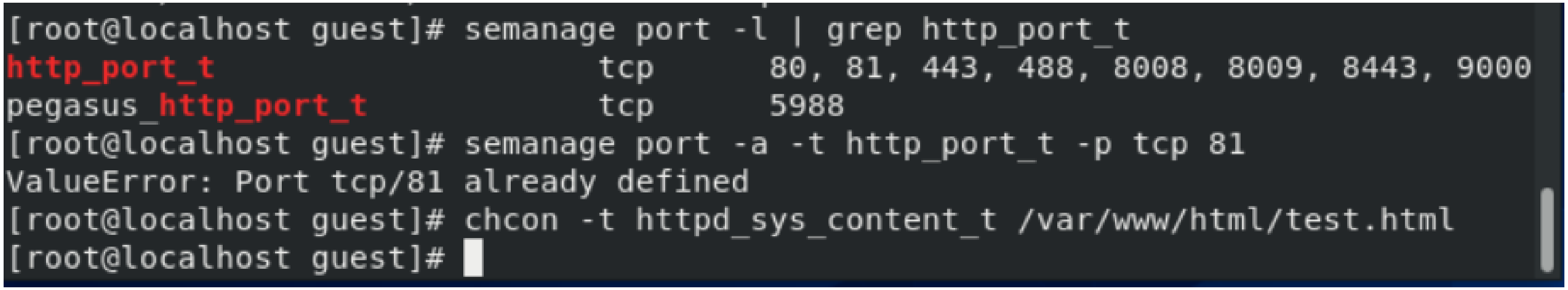
Выполнение лабораторной работы



```
[root@localhost guest]# 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@localhost guest]#
```

Порт 81

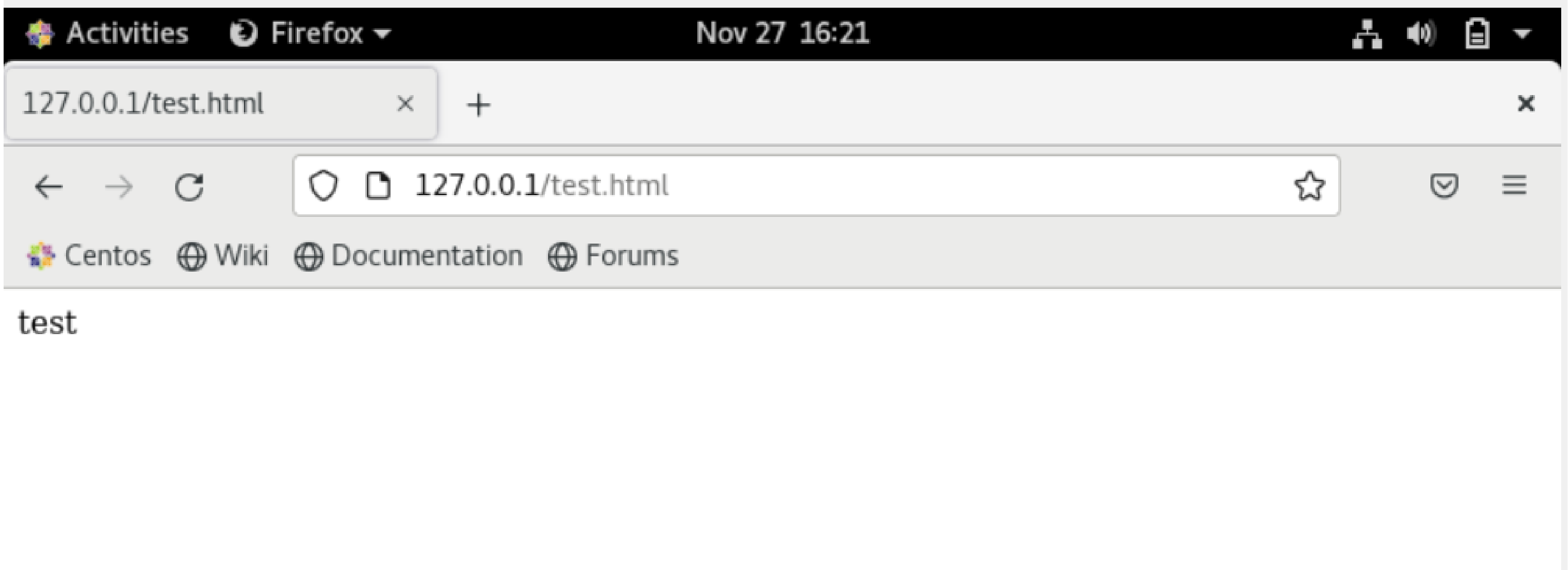
Выполнение лабораторной работы



```
[root@localhost guest]# 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@localhost guest]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost guest]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@localhost guest]# 
```

Контекст файла test

Выполнение лабораторной работы



test

Контекст файла test

ВЫВОД

Вывод

В процессе выполнения лабораторной работы мы развили навыков администрирования ОС Linux, а также освоили технологии SELinux. Мы проверили работу SELinux совместно с веб-сервером Apache.