

Презентация по лабораторной работе №6

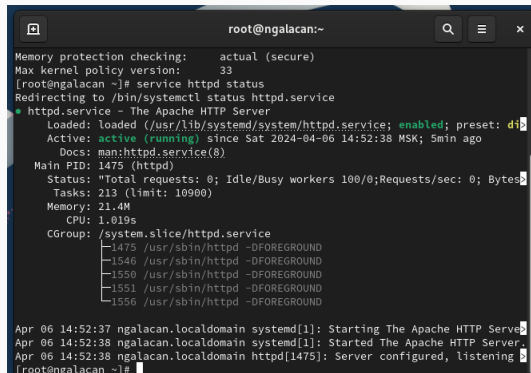
Мандатное разграничение прав в Linux

Галацан Николай

Российский университет дружбы народов, Москва, Россия

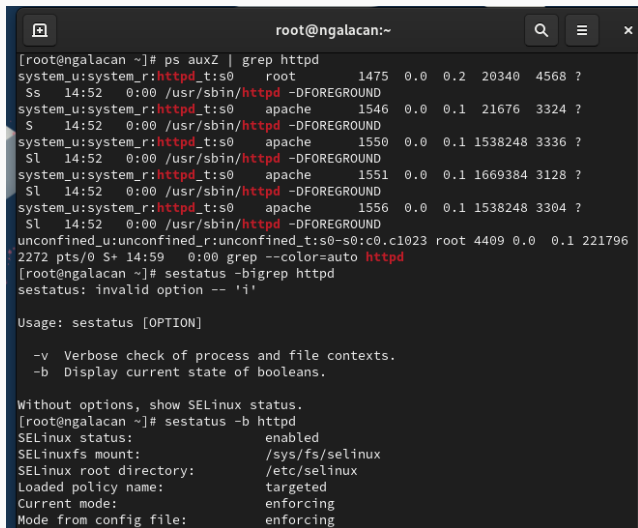
- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

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



```
root@ngalacan:~  
Memory protection checking:    actual (secure)  
Max kernel policy version:    33  
[root@ngalacan ~]# 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; preset: disabled)  
   Active: active (running) since Sat 2024-04-06 14:52:38 MSK; 5min ago  
     Docs: man:httpd.service(8)  
  Main PID: 1475 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0/0"  
    Tasks: 213 (limit: 10900)  
   Memory: 21.4M  
      CPU: 1.019s  
   CGroup: /system.slice/httpd.service  
            └─1475 /usr/sbin/httpd -DFOREGROUND  
              └─1546 /usr/sbin/httpd -DFOREGROUND  
                └─1550 /usr/sbin/httpd -DFOREGROUND  
                  └─1551 /usr/sbin/httpd -DFOREGROUND  
                    └─1556 /usr/sbin/httpd -DFOREGROUND  
  
Apr 06 14:52:37 ngalacan.localdomain systemd[1]: Starting The Apache HTTP Server:  
Apr 06 14:52:38 ngalacan.localdomain systemd[1]: Started The Apache HTTP Server.  
Apr 06 14:52:38 ngalacan.localdomain httpd[1475]: Server configured, listening on: 0.0.0.0:80  
[root@ngalacan ~]#
```

Рис. 1: Режим работы SELinux, статус httpd



```
root@ngalacan:~  
[root@ngalacan ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 1475 0.0 0.2 20340 4568 ?  
Ss 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1546 0.0 0.1 21676 3324 ?  
S 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1550 0.0 0.1 1538248 3336 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1551 0.0 0.1 1669384 3128 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 1556 0.0 0.1 1538248 3304 ?  
Sl 14:52 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4409 0.0 0.1 221796  
2272 pts/0 S+ 14:59 0:00 grep --color=auto httpd  
[root@ngalacan ~]# 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@ngalacan ~]# 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
```

Выполнение лабораторной работы

```
[root@ngalacan ~]# 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:        5135     Attributes:       259
Users:        8       Roles:           15
Booleans:     357     Cond. Expr.:     390
Allow:        65409    Neverallow:      0
Auditallow:   172     Dontaudit:       8647
Type_trans:   267813  Type_change:     94
Type_member:  37      Range_trans:     6164
Role allow:   39      Role_trans:      419
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:         665
Netifcon:     0      Nodecon:         0

[root@ngalacan ~]#
```

Рис. 3: Статистика по политике

```
neticon. 0 nodecon. 0
[root@ngalacan ~]# 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
[root@ngalacan ~]# ls -lZ /var/www/html
total 0
[root@ngalacan ~]# mcedit /var/www/html/test.html

[root@ngalacan ~]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 Apr 6 1
5:09 test.html
[root@ngalacan ~]#
```

Рис. 4: Просмотр файлов, создание test.html и просмотр контекста

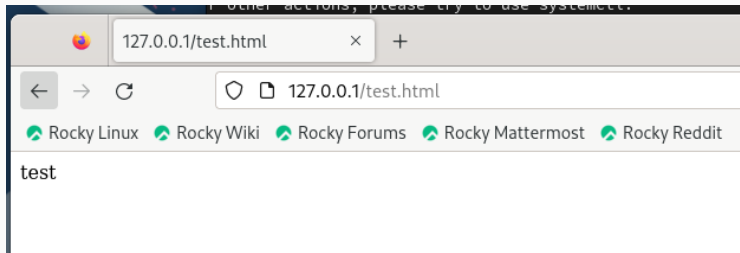


Рис. 5: Запуск файла в браузере

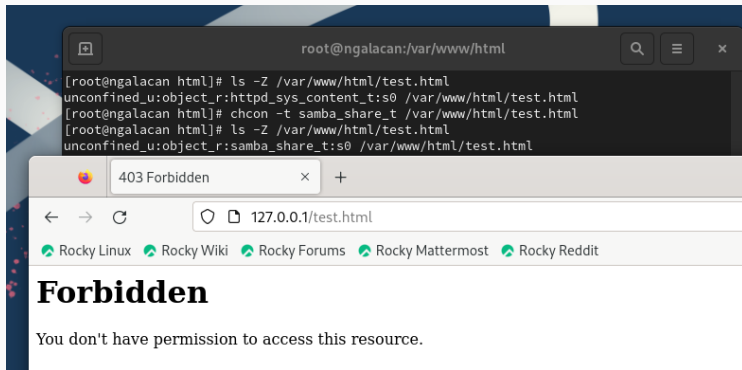
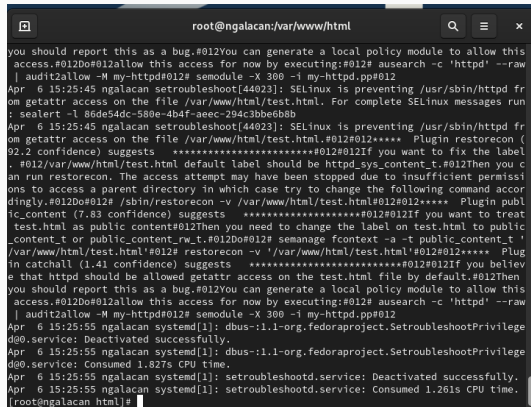


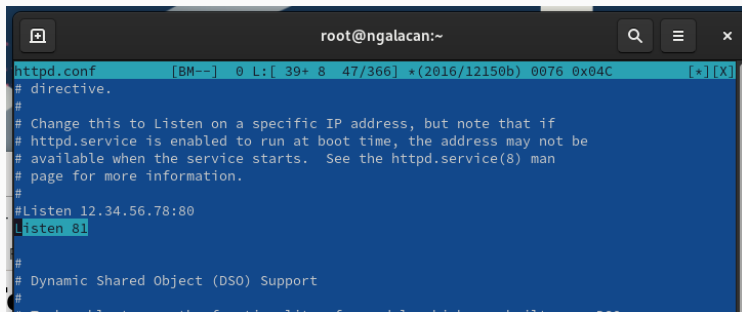
Рис. 6: Изменение контекста файла и попытка просмотра



```
root@ngalacan:/var/www/html

you should report this as a bug.#012You can generate a local policy module to allow this
access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw
| audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr  6 15:25:45 ngalacan setroubleshoot[44023]: SELinux is preventing /usr/sbin/httpd fr
om getattr access on the file /var/www/html/test.html. For complete SELinux messages run
: sealert -l 86de54dc-580e-4b4f-aeec-294c3bbe6b8b
Apr  6 15:25:45 ngalacan setroubleshoot[44023]: SELinux is preventing /usr/sbin/httpd fr
om getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (
92.2 confidence) suggests      *****#012#012If you want to fix the label
. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you c
an run restorecon. The access attempt may have been stopped due to insufficient permissi
ons to access a parent directory in which case try to change the following command accor
dingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin publ
ic_content (7.83 confidence) suggests      *****#012#012If you want to treat
test.html as public_content#012Then you need to change the label on test.html to public
_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***** Plug
in catchall (1.41 confidence) suggests      *****#012#012If you believ
e that httpd should be allowed getattr access on the test.html file by default.#012Then
you should report this as a bug.#012You can generate a local policy module to allow this
access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw
| audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr  6 15:25:55 ngalacan systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
d@0.service: Deactivated successfully.
Apr  6 15:25:55 ngalacan systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
d@0.service: Consumed 1.827s CPU time.
Apr  6 15:25:55 ngalacan systemd[1]: setroubleshootd.service: Deactivated successfully.
Apr  6 15:25:55 ngalacan systemd[1]: setroubleshootd.service: Consumed 1.261s CPU time.
[root@ngalacan html]#
```

Рис. 7: Просмотр лог-файла



```
root@ngalacan:~  
httpd.conf [BM--] 0 L:[ 39+ 8 47/366] *(2016/12150b) 0076 0x04C [*] [X]  
# 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
```

Рис. 8: Изменение порта в конфигурационном файле

Выполнение лабораторной работы

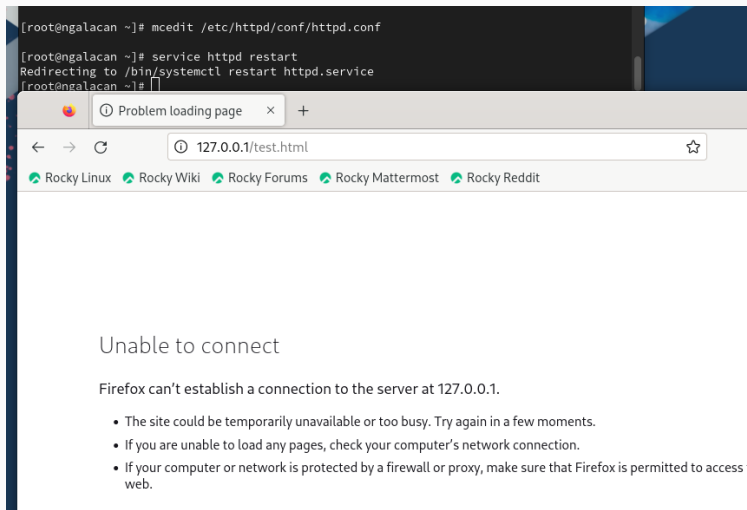


Рис. 9: Сбой веб-сервера

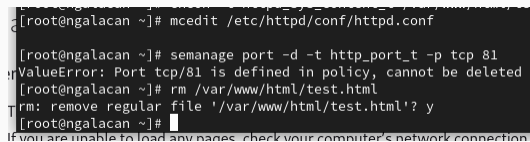
```
[root@ngalacan ~]# tail -nl /var/log/messages
tail: invalid number of lines: 'l'
[root@ngalacan ~]# tail -10l /var/log/messages
Apr  6 15:25:55 ngalacan systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
d@0.service: Consumed 1.827s CPU time.
Apr  6 15:25:55 ngalacan systemd[1]: setroubleshootd.service: Deactivated successfully.
Apr  6 15:25:55 ngalacan systemd[1]: setroubleshootd.service: Consumed 1.261s CPU time.
Apr  6 15:31:58 ngalacan systemd[1]: Stopping The Apache HTTP Server...
Apr  6 15:31:59 ngalacan systemd[1]: httpd.service: Deactivated successfully.
Apr  6 15:31:59 ngalacan systemd[1]: Stopped The Apache HTTP Server.
Apr  6 15:31:59 ngalacan systemd[1]: httpd.service: Consumed 1.622s CPU time.
Apr  6 15:31:59 ngalacan systemd[1]: Starting The Apache HTTP Server...
Apr  6 15:32:00 ngalacan httpd[44186]: Server configured, listening on: port 81
Apr  6 15:32:00 ngalacan systemd[1]: Started The Apache HTTP Server.
[root@ngalacan ~]# less /var/log/audit/audit.log
[root@ngalacan ~]#
```

Рис. 10: Просмотр лог-файла

Выполнение лабораторной работы

```
root@ngalacan:~  
[root@ngalacan ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ngalacan ~]# 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@ngalacan ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ngalacan ~]# 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; preset: disabled)  
   Active: active (running) since Sat 2024-04-06 15:35:46 MSK; 21s ago  
     Docs: man:httpd.service(8)  
  Main PID: 44467 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"  
    Tasks: 213 (limit: 10900)  
  Memory: 29.2M  
    CPU: 141ms  
   CGroup: /system.slice/httpd.service  
           └─44467 /usr/sbin/httpd -DFOREGROUND  
             └─44471 /usr/sbin/httpd -DFOREGROUND  
               └─44472 /usr/sbin/httpd -DFOREGROUND  
                 └─44473 /usr/sbin/httpd -DFOREGROUND  
                   └─44474 /usr/sbin/httpd -DFOREGROUND  
  
Apr 06 15:35:46 ngalacan.localdomain systemd[1]: Starting The Apache HTTP Server...  
Apr 06 15:35:46 ngalacan.localdomain httpd[44467]: Server configured, listening on: port 81  
Apr 06 15:35:46 ngalacan.localdomain systemd[1]: Started The Apache HTTP Server.  
[root@ngalacan ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ngalacan ~]# ls -Z /var/www/html/test.html  
ls: invalid option -- '/'  
Try 'ls --help' for more information.  
[root@ngalacan ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@ngalacan ~]#
```

Рис. 11: Добавление порта 81 и проверка. Перезапуск веб-сервера. Возвращение контекста

A terminal window with a dark background and light-colored text. The prompt is [root@ngalacan ~]. The user enters 'mcedit /etc/httpd/conf/httpd.conf'. The prompt changes to [root@ngalacan ~]#. The user enters 'semanage port -d -t http_port_t -p tcp 81'. The terminal shows an error: 'ValueError: Port tcp/81 is defined in policy, cannot be deleted'. The user enters 'rm /var/www/html/test.html'. The terminal shows the command being executed: 'rm: remove regular file '/var/www/html/test.html'? y'. The user enters '#'. The terminal shows the prompt [root@ngalacan ~]#. Below the terminal window, there is a line of text: 'If you are unable to load any pages, check your computer's network connection.'

```
[root@ngalacan ~]# mcedit /etc/httpd/conf/httpd.conf
[root@ngalacan ~]# semmanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@ngalacan ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@ngalacan ~]#
```

If you are unable to load any pages, check your computer's network connection.

Рис. 12: Завершение выполнения работы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux.
Проверена работа SELinux на практике совместно с веб-сервером Apache.