

Мандатное разграничение прав в Linux

Косолапов Степан ¹

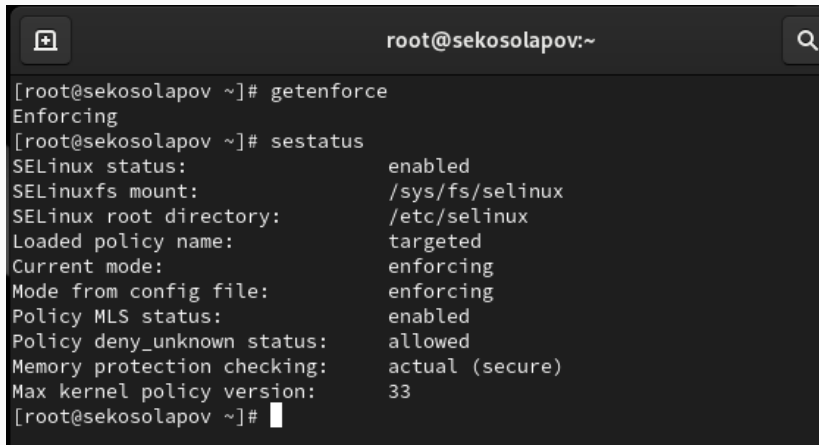
14 октября, 2023, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

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

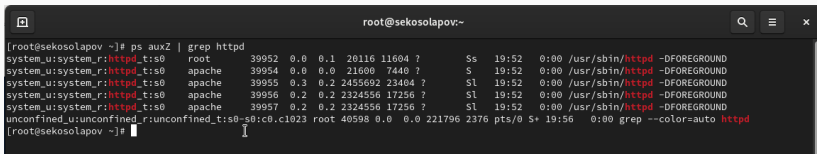
Процесс выполнения лабораторной работы



```
root@sekosolapov:~  
[root@sekosolapov ~]# getenforce  
Enforcing  
[root@sekosolapov ~]# 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@sekosolapov ~]#
```

Рис. 1: getenforce и sestatus

Контекст безопасности процессов httpd



```
root@sekosolapov:~  
[root@sekosolapov ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 39952 0.0 0.1 20116 11604 ? Ss 19:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 39954 0.0 0.0 21600 7440 ? S 19:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 39955 0.3 0.2 2455692 23404 ? Sl 19:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 39956 0.2 0.2 2324556 17256 ? Sl 19:52 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 39957 0.2 0.2 2324556 17256 ? Sl 19:52 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-c0:c0:c0:c0 root 40598 0.0 0.0 221796 2376 pts/0 S+ 19:56 0:00 grep --color=auto httpd  
[root@sekosolapov ~]#
```

Рис. 2: контекст безопасности процессов httpd

root@sekosolapov:~

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

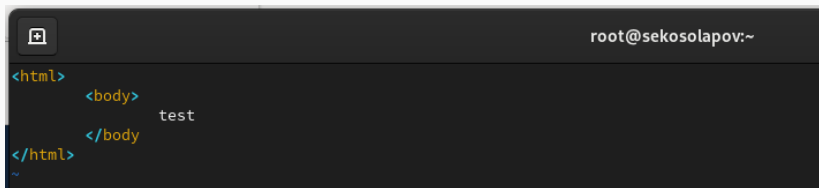
Classes:      135      Permissions:      457
Sensitivities:    1      Categories:      1024
Types:          5100    Attributes:       258
Users:          8       Roles:           14
Booleans:       353     Cond. Expr.:     384
Allow:          65009    Neverallow:      0
Auditallow:     170     Dontaudit:       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
Auditallowxperm: 0      Dontauditxperm:  0
Ibendportcon:   0       Ibpkeycon:       0
Initial SIDs:   27      Fs_use:          35
Genfscon:       109     Portcon:         660
Netifcon:       0       Nodecon:         0
```

```
[root@sekosolapov ~]#
```

```
[root@sekosolapov ~]# ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
```

Рис. 4: данные о содержимом /var/www/

Создание тестового html файла



A terminal window with a dark background. The title bar shows a window icon on the left and the text "root@sekosolapov:~" on the right. The terminal content shows the creation of an HTML file:

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

Рис. 5: test.html

Контекст созданных файлов

```
[root@sekosolapov ~]# vim /var/www/html/test.html
[root@sekosolapov ~]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 38 Oct 14 20:02 test.html
[root@sekosolapov ~]# ls --lcontext /var/www/html/
ls: unrecognized option '--lcontext'
Try 'ls --help' for more information.
[root@sekosolapov ~]# ls -l --context /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 38 Oct 14 20:02 test.html
[root@sekosolapov ~]#
```

Рис. 6: контекст test.html

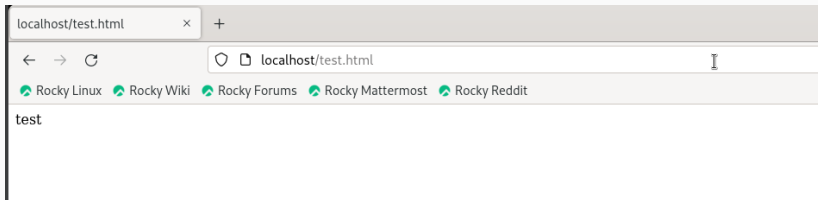
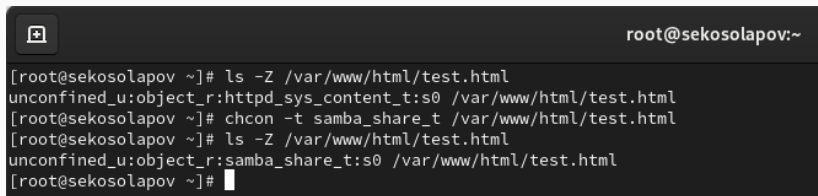


Рис. 7: test.html в браузере



A terminal window with a dark background. The title bar shows a window icon on the left and the text 'root@sekosolapov:~' on the right. The terminal contains the following text:

```
[root@sekosolapov ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@sekosolapov ~]# chcon -t samba_share_t /var/www/html/test.html
[root@sekosolapov ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@sekosolapov ~]#
```

Рис. 8: смена контекста

Ошибки при доступе к файлу с изменённым контекстом

```
ml. For complete SELinux messages run: sealert -l 6a31ec24-1cc2-4114-be59-a28f4aa42071
Oct 14 20:15:53 sekosolapov setroubleshoot[41308]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.ht
ml. #012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/ht
ml/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insu
fficient permissions to access a parent directory in 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 te
st.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 fc
ontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confi
dence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default
t.#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
Oct 14 20:16:03 sekosolapov systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 14 20:16:03 sekosolapov systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.186s CPU time.
Oct 14 20:16:04 sekosolapov systemd[1]: setroubleshoold.service: Deactivated successfully.
[root@sekosolapov ~]#
```

Рис. 9: системные логи

Прослушивание порта не в http_port_t

```
[root@sekosolapov ~]# 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@sekosolapov ~]# semanage port -a -t http_port_t -p tcp 82
[root@sekosolapov ~]# semanage port -l | grep http_port_t
http_port_t          tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@sekosolapov ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@sekosolapov ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@sekosolapov ~]# wget localhost:81/test.html
--2023-10-14 20:31:29-- http://localhost:81/test.html
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:81... failed: Connection refused.
Connecting to localhost (localhost)|127.0.0.1|:81... failed: Connection refused.
[root@sekosolapov ~]# wget localhost:82/test.html
--2023-10-14 20:31:35-- http://localhost:82/test.html
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:82... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38 [text/html]
Saving to: 'test.html'

test.html                               100%[=====]

2023-10-14 20:31:35 (5.67 MB/s) - 'test.html' saved [38/38]

[root@sekosolapov ~]# wget localhost:82/test.html | cat
```

Выводы по проделанной работе

В данной работе мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.