Мандатное разграничение прав в Linux

Лабораторная работа № 6

Абу Сувейлим М. М.

10 января 2003

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Абу Сувейлим Мухаммед Мунифович
- Студент
- Российский университет дружбы народов
- 1032215135@pfur.ru
- https://mukhammed-abu-suveilim.github.io/

Вводная часть

Цели и задачи

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

Материалы и методы

- Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.

Выполнение лабораторной работы

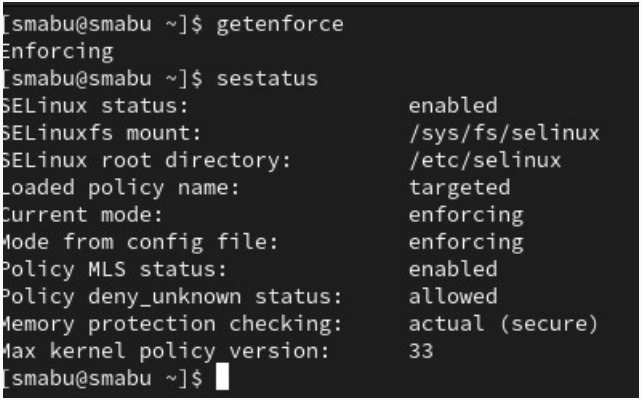

Figure 1: Коианда getenforce

Коианда service httpd status

```
[smabu@smabu ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-10-12 14:07:48 MSK; 1min 3s ago
       Docs: man:httpd.service(8)
   Main PID: 47128 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 47881)
     Memory: 21.8M
        CPU: 67ms
     CGroup: /system.slice/httpd.service
             ├─47128 /usr/sbin/httpd -DFOREGROUND
             ├─47129 /usr/sbin/httpd -DFOREGROUND
             ├─47134 /usr/sbin/httpd -DFOREGROUND
             ├─47135 /usr/sbin/httpd -DFOREGROUND
             └─47136 /usr/sbin/httpd -DFOREGROUND
[smabu@smabu ~]$
```

Figure 2: Коианда service httpd status

Коианда ps -eZ | grep httpd

```
[root@smabu httpd]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      47128 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      47129 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      47134 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      47135 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      47136 ?        00:00:00 httpd
[root@smabu httpd]#
```

Figure 3: Коианда ps -eZ | grep httpd

Коианда sestatus -b | grep httpd

```
[root@smabu httpd]# 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
httpd_graceful_shutdown                     off
httpd_manage_ipa                            off
httpd_mod_auth_ntlm_winbind                 off
httpd_mod_auth_pam                          off
httpd_read_user_content                     off
httpd_run_ipa                               off
httpd_run_preupgrade                        off
httpd_run_stickshift                        off
httpd_serve_cobbler_files                   off
httpd_setrlimit                             off
httpd_ssi_exec                              off
httpd_sys_script_anon_write                 off
httpd_tmp_exec                              off
httpd_tty_comm                              off
httpd_unified                               off
httpd_use_cifs                              off
httpd_use_fusefs                            off
httpd_use_gpg                               off
httpd_use_nfs                               off
httpd_use_opencryptoki                      off
httpd_use_openstack                         off
httpd_use_sasl                              off
httpd_verify_dns                            off
```

Коианда seinfo

```
[root@smabu httpd]# 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:              5169    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            358    Cond. Expr.:         390
  Allow:             65633    Neverallow:            0
  Auditallow:          176    Dontaudit:          8703
  Type_trans:       271851    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  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@smabu httpd]#
```

Figure 5: Коианда seinfo

Коианда ls -lZ /var/www

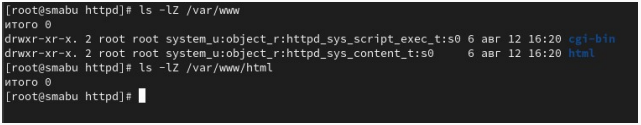

Figure 6: Коианда ls -lZ /var/www

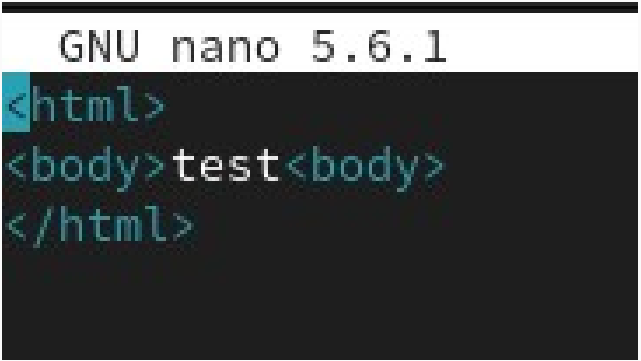

Figure 7: html-файл test.html

html-файл test.html 2

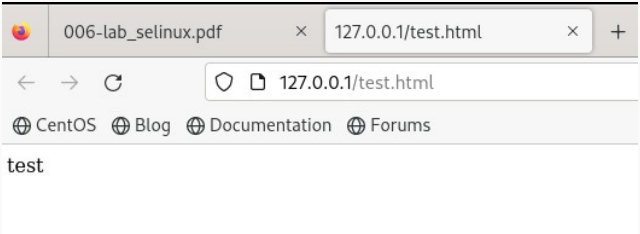

Figure 8: html-файл test.html 2

Коианда man httpd

```
HTTPD(8)                                httpd                                HTTPD(8)

NAME
       httpd - Apache Hypertext Transfer Protocol Server

SYNOPSIS
       httpd  [  -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D parameter ] [ -e level ] [ -E
       file ] [ -k start|restart|graceful|stop|graceful-stop ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ]  [
       -X ] [ -M ] [ -T ]

       On Windows systems, the following additional arguments are available:

       httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
       httpd  is the Apache HyperText Transfer Protocol (HTTP) server program. It is designed to be run as a stand-
       alone daemon process. When used like this it will create a pool of child processes or threads to handle re-
       quests.

       In  general,  httpd should not be invoked directly, but rather should be invoked via apachectl on Unix-based
       systems or as a service on Windows NT, 2000 and XP and as a console application on Windows 9x and ME.

OPTIONS
       -d serverroot
              Set the initial value for the ServerRoot directive to serverroot.  This  can  be  overridden  by  the
              ServerRoot directive in the configuration file. The default is /etc/httpd.

       -f config
              Uses  the  directives  in  the  file config on startup. If config does not begin with a /, then it is
              taken to be a path relative to the ServerRoot. The default is conf/httpd.conf.

       -k start|restart|graceful|stop|graceful-stop
              Signals httpd to start, restart, or stop. See Stopping Apache httpd for more information.

       -C directive
              Process the configuration directive before reading config files.

       -c directive
              Process the configuration directive after reading config files.

       -D parameter
              Sets a configuration parameter which can be used with <IfDefine> sections in the configuration  files
              to conditionally skip or process commands at server startup and restart. Also can be used to set cer-
              tain less-common startup parameters including -DNO_DETACH  (prevent  the  parent  from  forking)  and
              -DFOREGROUND (prevent the parent from calling setsid() et al).

       -e level
              Sets  the LogLevel to level during server startup. This is useful for temporarily increasing the ver-
              bosity of the error messages to find problems during startup.

       -E file
              Send error messages during server startup to file.

       -h     Output a short summary of available command line options.

       -l     Output a list of modules compiled into the server. This will not list dynamically loaded modules  in-
              cluded using the LoadModule directive.
```

Коианда chcon

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

Figure 10: Коианда chcon

Ошибка Forbidden

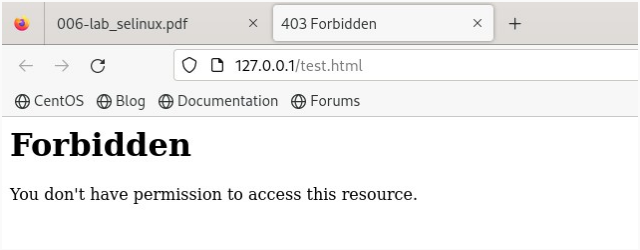

Figure 11: Ошибка Forbidden

Команда ls -l /var/www/html/test.html

Figure 12: Команда ls -l /var/www/html/test.html

Лог-файлы

Figure 13: Лог-файлы

Команда semanage

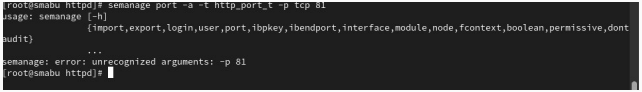

Figure 14: Команда semanage

Команда rm /var/www/html/test.html

```
[root@smabu httpd]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@smabu httpd]#
```

Figure 15: Команда rm /var/www/html/test.html

Выводы

Выводы

Развивли свои навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.