Презентация лабораторной работы №6

Мандатное разграничение прав в Linux

Тасыбаева Н.С.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цели и задачи работы

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

Результаты

```
Installed:
  apr-1.7.0-11.el9.x86_64
  apr-util-1.6.1-20.el9_2.1.x86_64
  apr-util-bdb-1.6.1-20.el9_2.1.x86_64
  apr-util-openssl-1.6.1-20.el9_2.1.x86_64
  httpd-2.4.53-11.el9_2.5.x86_64
  httpd-core-2.4.53-11.el9_2.5.x86_64
  httpd-filesystem-2.4.53-11.el9_2.5.noarch
  httpd-tools-2.4.53-11.el9_2.5.x86_64
  mod_http2-1.15.19-4.el9_2.4.x86_64
  mod_lua-2.4.53-11.el9_2.5.x86_64
  rocky-logos-httpd-90.14-1.el9.noarch

Complete!
[nstasihbaeva@nstasihbaeva ~]$ cat etc/httpd/httpd.conf
```

Рис. 1: Запуск сервера

Результаты

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru
```

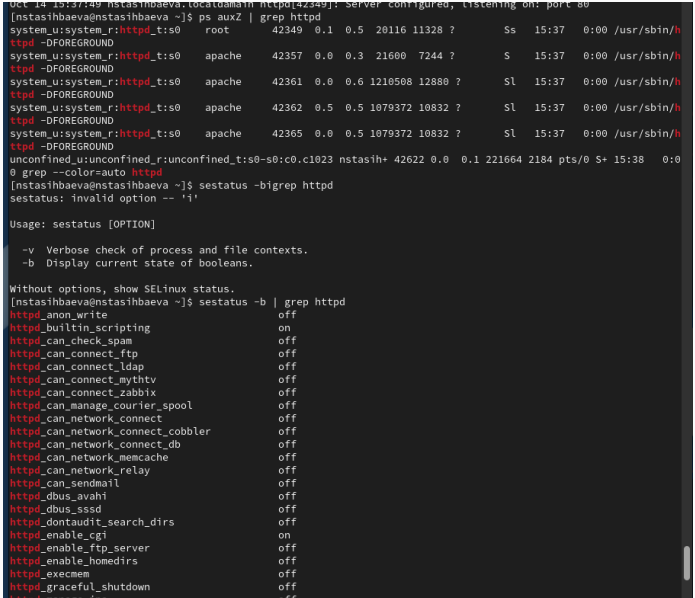
Рис. 2: Параметр ServerName

Результаты

```
[nstasihbaeva@nstasihbaeva ~]$ 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: inactive (dead)
       Docs: man:httpd.service(8)
[nstasihbaeva@nstasihbaeva ~]$ getenforce
Enforcing
[nstasihbaeva@nstasihbaeva ~]$ 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
[nstasihbaeva@nstasihbaeva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[nstasihbaeva@nstasihbaeva ~]$ 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 2023-10-14 15:37:49 MSK; 13s ago
       Docs: man:httpd.service(8)
   Main PID: 42349 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 213 (limit: 12224)
     Memory: 23.3M
        CPU: 447ms
     CGroup: /system.slice/httpd.service
             ├─42349 /usr/sbin/httpd -DFOREGROUND
             ├─42357 /usr/sbin/httpd -DFOREGROUND
             ├─42361 /usr/sbin/httpd -DFOREGROUND
             ├─42362 /usr/sbin/httpd -DFOREGROUND
             └─42365 /usr/sbin/httpd -DFOREGROUND

Oct 14 15:37:48 nstasihbaeva.localdamain systemd[1]: Starting The Apache HTTP Server...
Oct 14 15:37:49 nstasihbaeva.localdamain systemd[1]: Started The Apache HTTP Server.
Oct 14 15:37:49 nstasihbaeva.localdamain httpd[42349]: Server configured, listening on: port 80
```

Результаты


Oct 14 15:37:49 nstasihbaeva.localdomain httpd[42349]: Server configured, listening on: port 80
[nstasihbaeva@nstasihbaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42349 0.1 0.5 20116 11328 ? Ss 15:37 0:00 /usr/sbin/h
ttpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42357 0.0 0.3 21600 7244 ? S 15:37 0:00 /usr/sbin/h
ttpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42361 0.0 0.6 1210508 12880 ? Sl 15:37 0:00 /usr/sbin/h
ttpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42362 0.5 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/h
ttpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42365 0.0 0.5 1079372 10832 ? Sl 15:37 0:00 /usr/sbin/h
ttpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 nstasih+ 42622 0.0 0.1 221664 2184 pts/0 S+ 15:38 0:0
0 grep --color=auto httpd
[nstasihbaeva@nstasihbaeva ~]$ 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.
[nstasihbaeva@nstasihbaeva ~]$ 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

Результаты

```
* Installing packages...
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:             65000    Neverallow:            0
  Auditallow:          170    Dontaudit:          8572
  Type_trans:       265341    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

[nstasihbaeva@nstasihbaeva ~]$
```

Результаты

```
[nstasihbaeva@nstasihbaeva ~]$ 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
[nstasihbaeva@nstasihbaeva ~]$ ls -lZ /var/www/html
total 0
[nstasihbaeva@nstasihbaeva ~]$ cd /var/www
[nstasihbaeva@nstasihbaeva www]$ cd html
[nstasihbaeva@nstasihbaeva html]$ ls -lZ
total 0
[nstasihbaeva@nstasihbaeva html]$ ls -l
total 0
[nstasihbaeva@nstasihbaeva html]$ cd ../
[nstasihbaeva@nstasihbaeva www]$ ls -l
total 0
drwxr-xr-x. 2 root root 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root 6 May 16 23:21 html
[nstasihbaeva@nstasihbaeva www]$ sudo -i
[sudo] password for nstasihbaeva:
[root@nstasihbaeva ~]# cd /var/www/html
[root@nstasihbaeva html]# touch test.html
[root@nstasihbaeva html]# vi test.html
[root@nstasihbaeva html]# cat test.html
<html>
<body>test</body>
</html>

[root@nstasihbaeva html]# ls -l
total 4
-rw-r--r--. 1 root root 34 Oct 14 15:49 test.html
[root@nstasihbaeva html]# ls -lZ
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 14 15:49 test.html
[root@nstasihbaeva html]#
```


Рис. 6. Типы файлов и поддиректории

Результаты

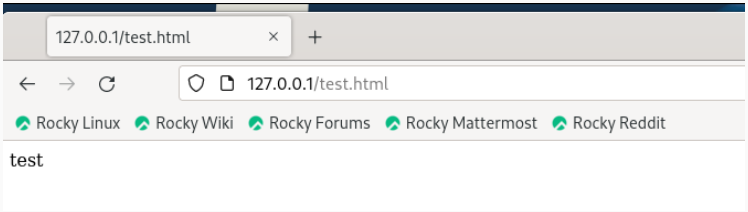


Рис. 7: Запуск в браузере

Результаты

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

Рис. 8: Изменение контеста безопасности

Результаты

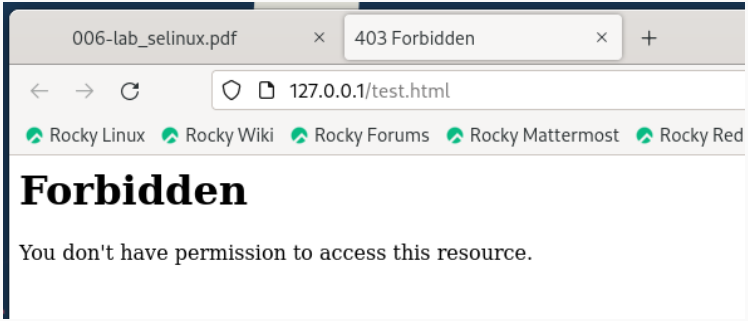


Рис. 9: Запуск в браузере с ошибкой

Результаты

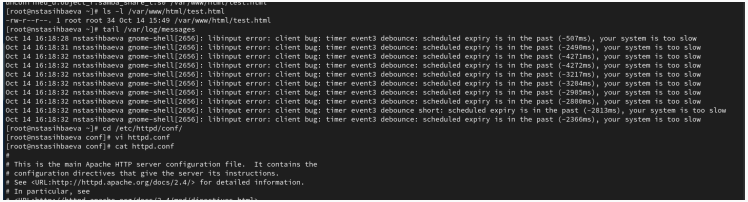


Рис. 10: Лог файлы

Результаты

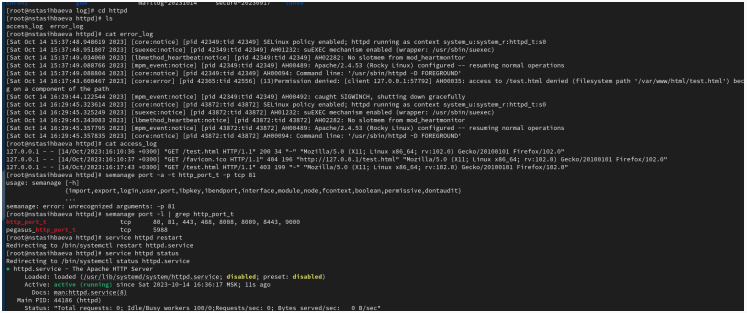


Рис. 11: Настройки

Результаты

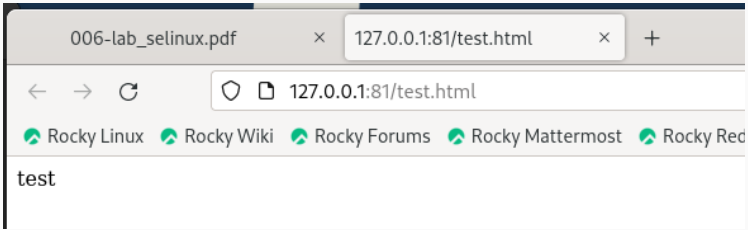


Рис. 12: Запуск в браузере

Результаты

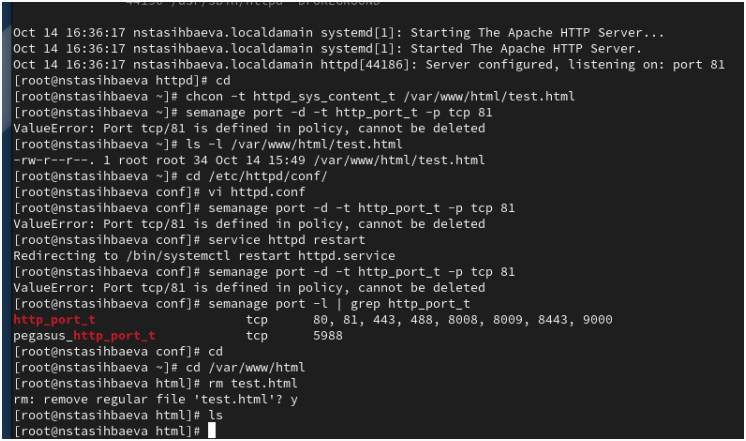


Рис. 13: Открытие файла

Выводы по проделанной работе

Выводы по проделанной работе

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.