Лабораторная работа № 6

Мандатное разграничение прав в Linux

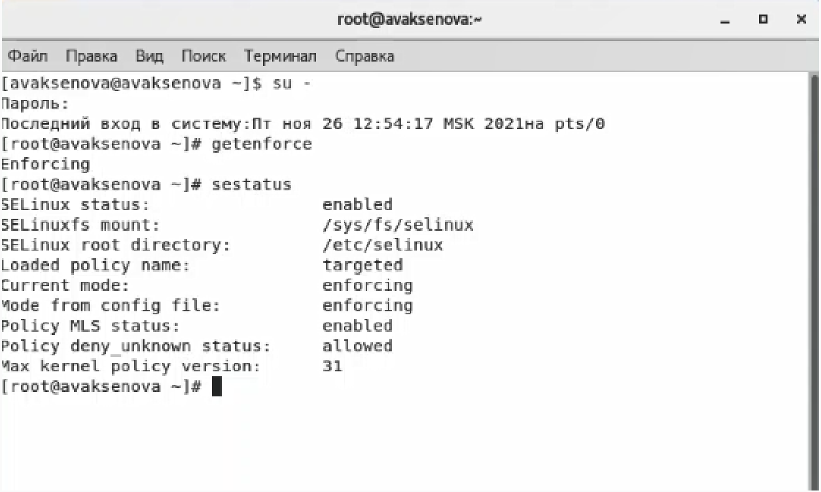
Аксёнова Алина Владимировна

Цель работы

Развить навыки администрирования ОС Linux.Проверить работу SELinx на практике совместно с веб-сервером Apache..

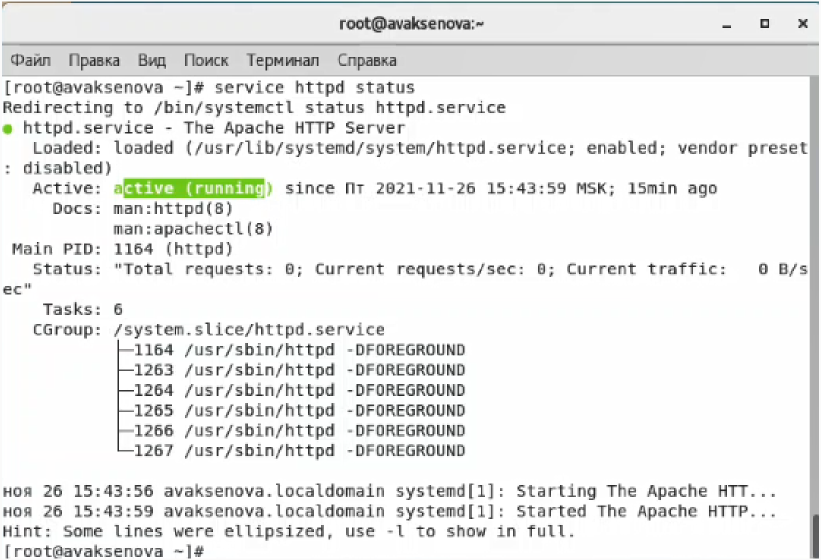
Ход работы

Вход в систему, проверка режима и политики



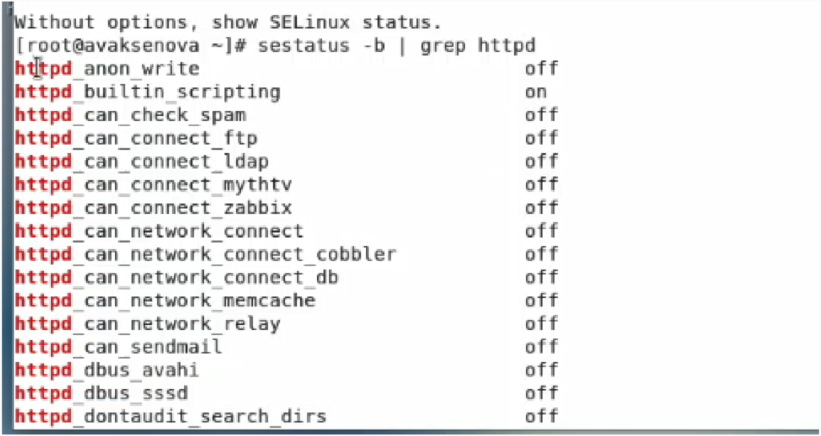
```
[avaksenova@avaksenova ~]$ su -
Пароль:
Последний вход в систему:Пт ноя 26 12:54:17 MSK 2021на pts/0
[root@avaksenova ~]# getenforce
Enforcing
[root@avaksenova ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
[root@avaksenova ~]#
```

Проверка работы веб-сервера



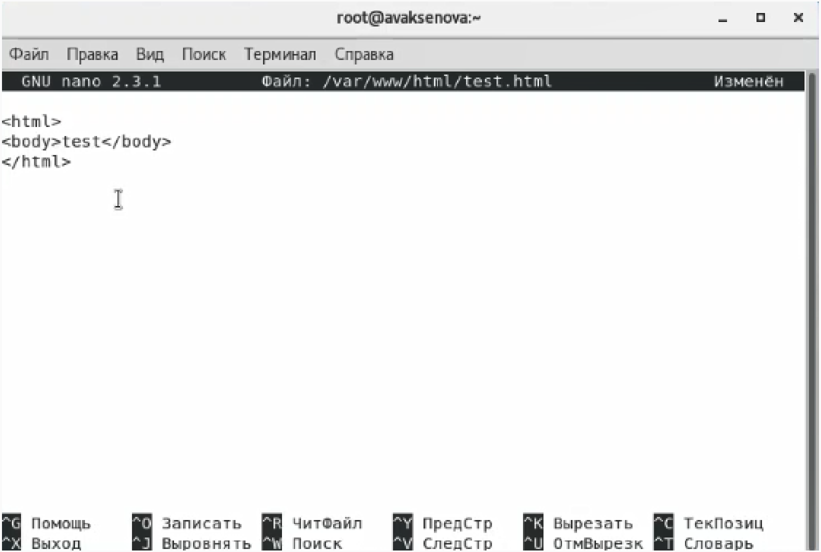
```
[root@avaksenova ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset
: disabled)
   Active: active (running) since Пт 2021-11-26 15:43:59 MSK; 15min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 1164 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/s
ec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─1164 /usr/sbin/httpd -DFOREGROUND
           ├─1263 /usr/sbin/httpd -DFOREGROUND
           ├─1264 /usr/sbin/httpd -DFOREGROUND
           ├─1265 /usr/sbin/httpd -DFOREGROUND
           ├─1266 /usr/sbin/httpd -DFOREGROUND
           └─1267 /usr/sbin/httpd -DFOREGROUND

ноя 26 15:43:56 avaksenova.localdomain systemd[1]: Starting The Apache HTT...
ноя 26 15:43:59 avaksenova.localdomain systemd[1]: Started The Apache HTTP...
Hint: Some lines were ellipsized, use -l to show in full.
[root@avaksenova ~]#
```

Состояние SELinux переключателей



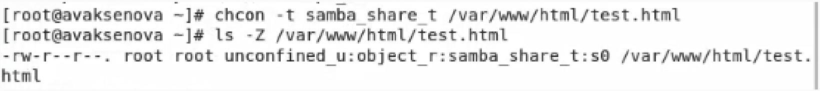
```
Without options, show SELinux status.
[root@avaksenova ~]# sestatus -b | grep httpd
httpd_anon_write                                 off
httpd_builtin_scripting                          on
httpd_can_check_spam                             off
httpd_can_connect_ftp                            off
httpd_can_connect_ldap                           off
httpd_can_connect_mythtv                         off
httpd_can_connect_zabbix                         off
httpd_can_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
```

Создание html-файла



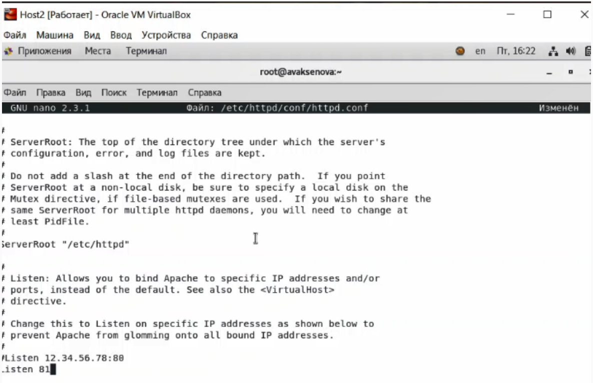
```
  GNU nano 2.3.1          Файл: /var/www/html/test.html                    Изменён

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













^G Помощь      ^O Записать    ^R ЧитФайл     ^Y ПредСтр     ^K Вырезать    ^C ТекПозиц
^X Выход       ^J Выровнять   ^W Поиск       ^V СледСтр     ^U ОтмВырезк   ^T Словарь
```

Смена контекста файла



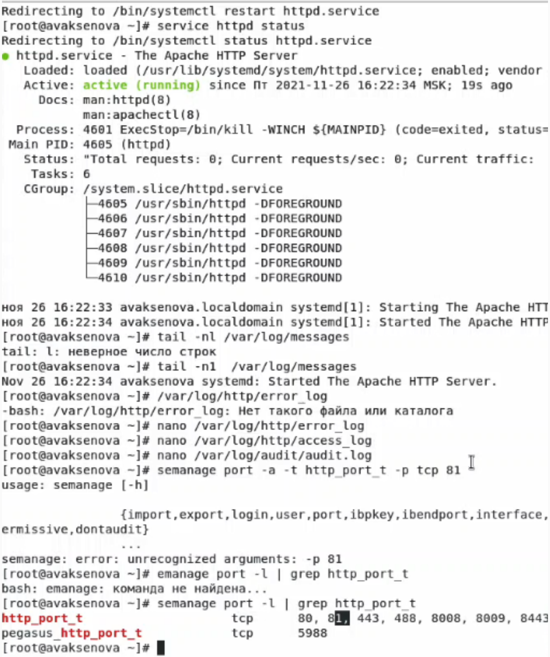
```
[root@avaksenova ~]# chcon -t samba_share_t /var/www/html/test.html
[root@avaksenova ~]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.
html
```

Запуск веб-сервера Apache на прослушивание TCP-порта 81


Host2 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал
en Пт, 16:22
root@avaksenova:~
Файл Правка Вид Поиск Терминал Справка

```
  GNU nano 2.3.1              Файл: /etc/httpd/conf/httpd.conf              Изменён

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Перезапуск веб-сервера, анализ log-файлов



```
Redirecting to /bin/systemctl restart httpd.service
[root@avaksenova ~]# 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
   Active: active (running) since Пт 2021-11-26 16:22:34 MSK; 19s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 4601 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=
 Main PID: 4605 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─4605 /usr/sbin/httpd -DFOREGROUND
           ├─4606 /usr/sbin/httpd -DFOREGROUND
           ├─4607 /usr/sbin/httpd -DFOREGROUND
           ├─4608 /usr/sbin/httpd -DFOREGROUND
           ├─4609 /usr/sbin/httpd -DFOREGROUND
           └─4610 /usr/sbin/httpd -DFOREGROUND

ноя 26 16:22:33 avaksenova.localdomain systemd[1]: Starting The Apache HTT
ноя 26 16:22:34 avaksenova.localdomain systemd[1]: Started The Apache HTTP
[root@avaksenova ~]# tail -nl /var/log/messages
tail: l: неверное число строк
[root@avaksenova ~]# tail -n1  /var/log/messages
Nov 26 16:22:34 avaksenova systemd: Started The Apache HTTP Server.
[root@avaksenova ~]# /var/log/http/error_log
-bash: /var/log/http/error_log: Нет такого файла или каталога
[root@avaksenova ~]# nano /var/log/http/error_log
[root@avaksenova ~]# nano /var/log/http/access_log
[root@avaksenova ~]# nano /var/log/audit/audit.log
[root@avaksenova ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]

                {import,export,login,user,port,ibpkey,ibendport,interface,
ermissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@avaksenova ~]# emanage port -l | grep http_port_t
bash: emanage: команда не найдена...
[root@avaksenova ~]# semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443
pegasus_http_port_t            tcp      5988
[root@avaksenova ~]# █
```

Вывод

- В результате выполнения данной работы была изучена технология SELinux, а также проверена работа SELinux с веб-сервером Apache.