

Лабораторная работа № 6

Мандатное разграничение прав в Linux

Логинов Сергей

НФИбд-01-18

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinux на практике совместно с веб-сервером Apache

Ход работы

```
guest@saloginov:~  
Файл Правка Вид Поиск Терминал Справка  
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  
[guest@saloginov ~]$ 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 prese  
   Active: active (running) since Thu 2021-11-18 23:44:10 MSK; 1 day 16h ago  
     Docs: man:httpd.service(8)  
  Main PID: 40651 (httpd)  
    Status: "Running, listening on: port 443, port 80"  
     Tasks: 213 (limit: 5839)  
    Memory: 12.0M  
    CGroup: /system.slice/httpd.service  
            └─40651 /usr/sbin/httpd -DFOREGROUND  
              └─40658 /usr/sbin/httpd -DFOREGROUND  
                └─40659 /usr/sbin/httpd -DFOREGROUND  
                  └─40660 /usr/sbin/httpd -DFOREGROUND  
                    └─40661 /usr/sbin/httpd -DFOREGROUND  
lines 1-14/14 (END)
```

Для начала убедились, что наша система готова к работе

Ход работы

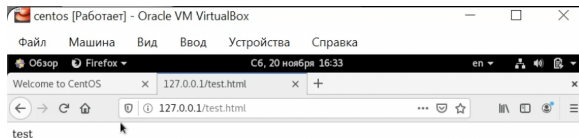
Создадим html-файл в директории /var

```
[guest@saloginov ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 18 23:48 html
[guest@saloginov ~]$ ls -lZ /var/www/html
итого 0
[guest@saloginov ~]$ su
Пароль:
[root@saloginov guest]# touch /var/www/html/test.html
[root@saloginov guest]#
```

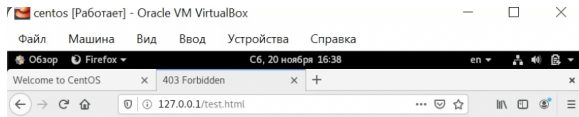
```
[root@saloginov guest]# vi /var/www/html/test.html
[root@saloginov guest]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@saloginov guest]# exit
exit
[guest@saloginov ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 20 16:31 test.html
```

Ход работы

Поработаем с файлом через браузер, изменим контекст



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

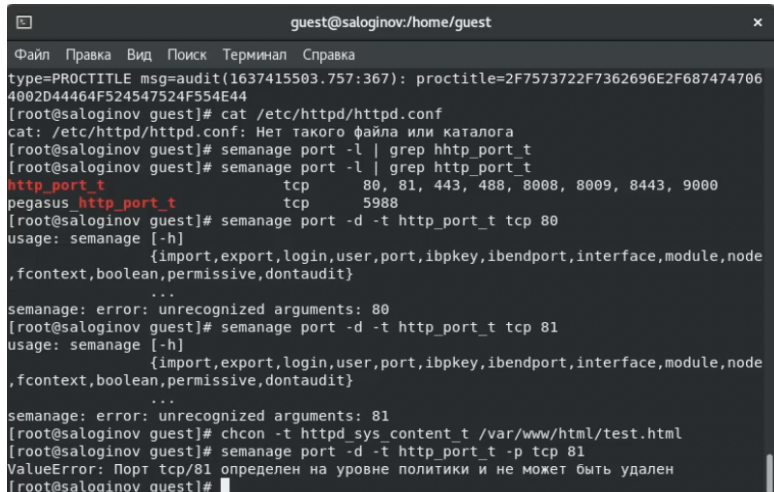


Forbidden

You don't have permission to access this resource.

Ход работы

При выполнении заданий с изменением ТСП-порта получили следующее



```
guest@saloginov:/home/guest
Файл Правка Вид Поиск Терминал Справка
type=PROCTITLE msg=audit(1637415503.757:367): proctitle=2F7573722F7362696E2F687474706
4002D44464F524547524F554E44
[root@saloginov guest]# cat /etc/httpd/httpd.conf
cat: /etc/httpd/httpd.conf: Нет такого файла или каталога
[root@saloginov guest]# semanage port -l | grep http_port_t
[root@saloginov guest]# 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@saloginov guest]# semanage port -d -t http_port_t tcp 80
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node
,fcontext,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 80
[root@saloginov guest]# semanage port -d -t http_port_t tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node
,fcontext,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 81
[root@saloginov guest]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@saloginov guest]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@saloginov guest]#
```

Вывод

В ходе лабораторной работы получили первое практическое знакомство с технологией SELinux и локальным веб-сервером Apache