

**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико–математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**Отчет по лабораторной работе № 6**

***Дисциплина: Информационная безопасность***

Студент: Логинов Сергей Андреевич

Группа: НФИбд-01-18

**МОСКВА 2021г**

## Цель работы

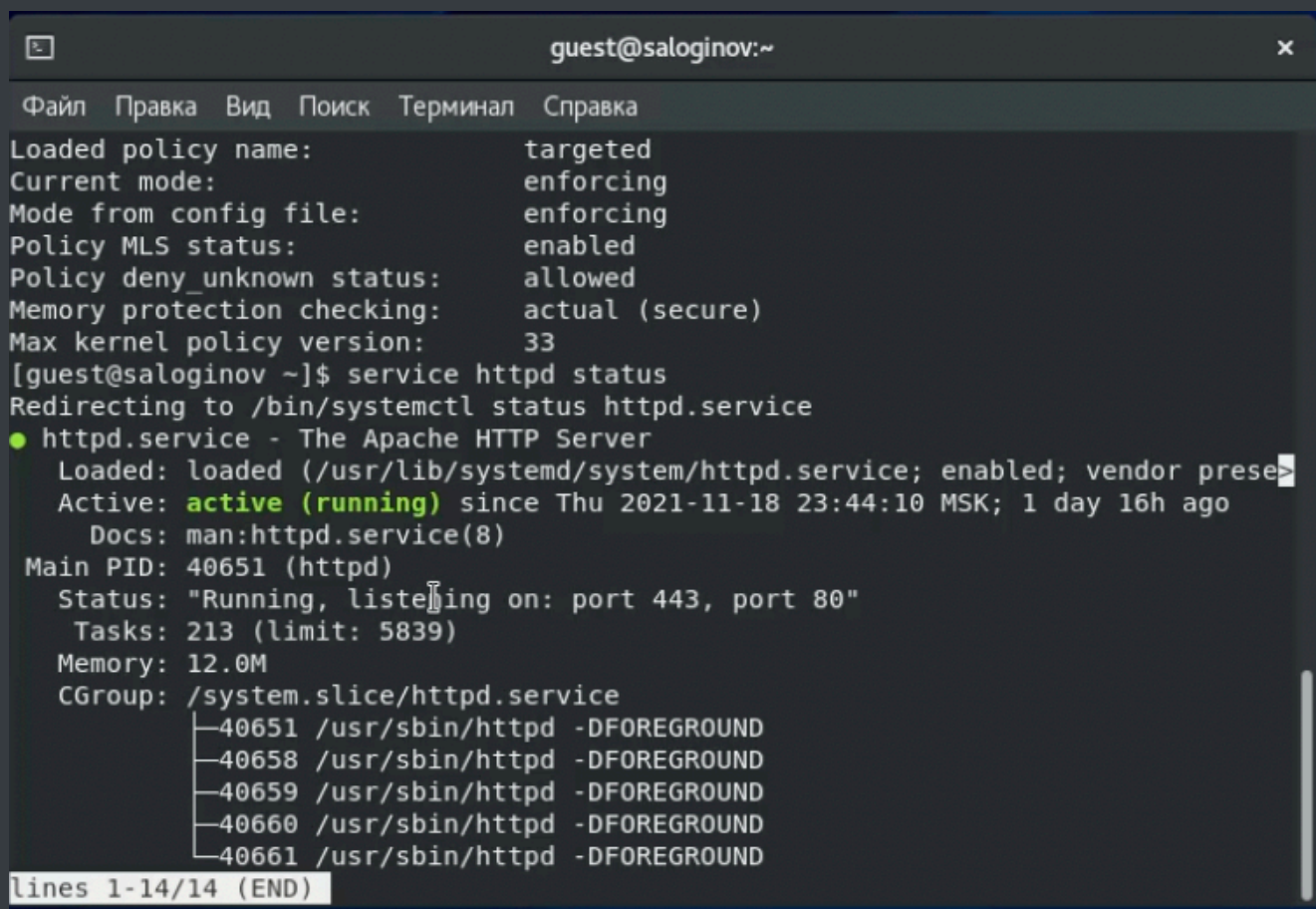
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Проверить работу SELinux на практике совместно с веб-сервером Apache.

## Ход работы

Были выполнены подготовительные процедуры и установлены необходимые пакеты.

1. Убедились, что SELinux работает в режиме enforcing политики targeted
2. С помощью веб-браузера обратились к локальному веб-серверу и убедились, что он работает



```
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)
```

3. Нашли веб-сервер Apache в списке процессов, контекст безопасности: system\_u:system\_r:httpd\_t:s0

```
guest@saloginov:~  
Файл Правка Вид Поиск Терминал Справка  
└─40661 /usr/sbin/httpd -DFOREGROUND  
[guest@saloginov ~]$ ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 40651 0.0 0.3 288588 3036 ? S  
16:07 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 40658 0.0 0.1 302468 1628 ? S  
16:07 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 40659 0.0 0.2 1360284 2100 ? S  
16:07 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 40660 0.0 0.1 1491412 1936 ? S  
16:07 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 40661 0.0 0.2 1360284 2104 ? S  
16:07 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 guest 41728 0.0 0.1 12136 1  
pts/0 R+ 16:26 0:00 grep --color=auto httpd  
[guest@saloginov ~]$ 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.  
[guest@saloginov ~]$ sestatus -
```

4. Проверили текущее состояние переключателей SELinux для Apache

```

[icon] guest@saloginov:~
Файл  Правка  Вид  Поиск  Терминал  Справка
secure_mode_insmode      off
secure_mode_policyload   off
selinuxuser_direct_dri_enabled  on
selinuxuser_execheap     off
selinuxuser_execmod      on
selinuxuser_execstack    on
selinuxuser_mysql_connect_enabled  off
selinuxuser_ping         on
selinuxuser_postgresql_connect_enabled  off
selinuxuser_rw_noexecattrfile  on
selinuxuser_share_music   off
selinuxuser_tcp_server    off
selinuxuser_udp_server    off
selinuxuser_use_ssh_chroot  off
sge_domain_can_network_connect  off
sge_use_nfs               off
smartmon_3ware            off
smbd_anon_write           off
spamassassin_can_network  off
spamd_enable_home_dirs    on
spamd_update_can_network  off
squid_connect_any         on
squid_use_tproxy          off
ssh_chroot_rw_homedirs    off

```

Действительно, большая часть переключателей находится в положении off



5. Посмотрели статистику по политике. Множество пользователей: 8, ролей: 14, типов: 4958

```
guest@saloginov:~  
Файл Правка Вид Поиск Терминал Справка  
zoneminder_run_sudo off  
[guest@saloginov ~]$ seinfo  
Statistics for policy file: /sys/fs/selinux/policy  
Policy Version: 31 (MLS enabled)  
Target Policy: selinux  
Handle unknown classes: allow  
Classes: 132 Permissions: 463  
Sensitivities: 1 Categories: 1024  
Types: 4958 Attributes: 255  
Users: 8 Roles: 14  
Booleans: 340 Cond. Expr.: 389  
Allow: 112830 Neverallow: 0  
Auditallow: 166 Dontaudit: 10362  
Type_trans: 252747 Type_change: 87  
Type_member: 35 Range_trans: 6015  
Role_allow: 37 Role_trans: 423  
Constraints: 72 Validatetrans: 0  
MLS Constrain: 72 MLS Val. Tran: 0  
Permissives: 0 Polcap: 5  
Defaults: 7 Typebounds: 0  
Allowxperm: 0 Neverallowxperm: 0  
Auditallowxperm: 0 Dontauditxperm: 0  
Ibendportcon: 0 Ibkeycon: 0  
Initial SIDs: 27 Fs_use: 33
```

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www
7. В директории /var/www/html отсутствуют какие-либо файлы
8. В данной директории файлы создавать может только владелец
9. От имени суперпользователя создали html-файл следующего содержания:

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

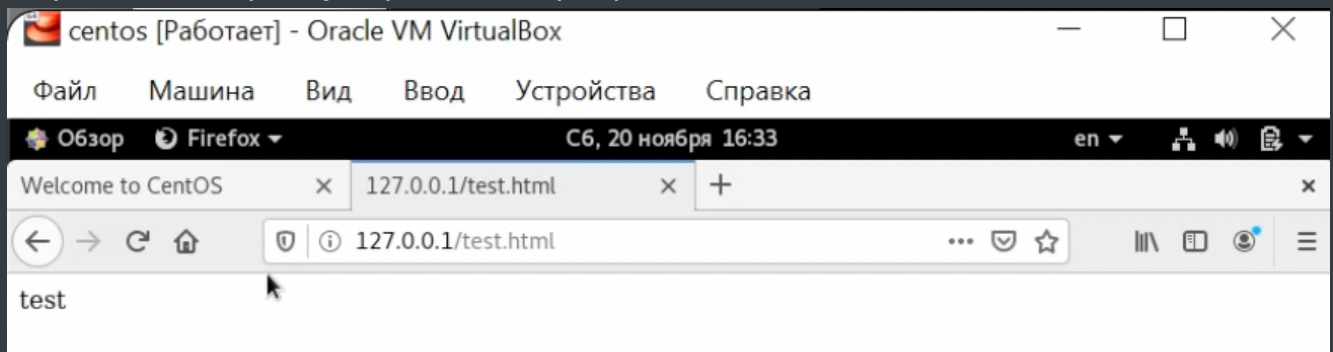
```
[guest@saloginov ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 c  
gi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 18 23:48 h  
tml  
[guest@saloginov ~]$ ls -lZ /var/www/html  
итого 0  
[guest@saloginov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

10. Проверили контекст созданного файла:

unconfined\_u:object\_r:httpd\_sys\_content\_t:s0

```
[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
```

11. Обратились к файлу через веб-сервер

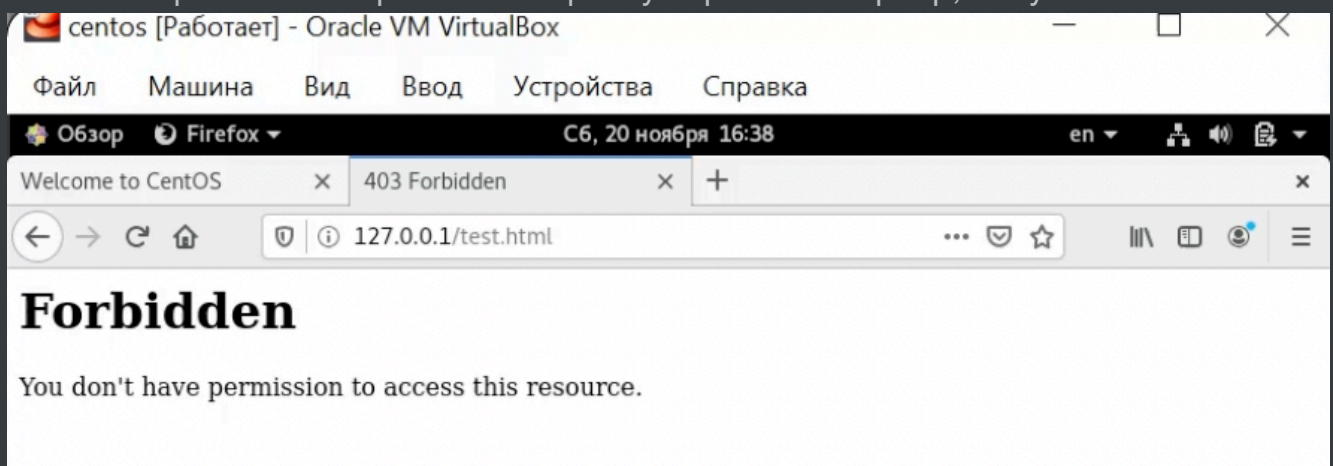


12. Изучили справку SELinux

13. Изменили контекст файла с httpd\_sys\_content\_t на samba\_share\_t

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

14. Снова попробовали обратиться к файлу через веб-сервер, получили отказ



15. Несмотря на то, что права доступа дают возможность читать файл любому пользователю, обратиться к нему через браузер не получилось, поскольку на файл был установлен другой контекст. Тип samba\_share\_t не позволяет процессу httpd получить доступ к файлу при обращении через браузер

Логи:

```
guest@saloginov:/home/guest
Файл Правка Вид Поиск Терминал Справка
e -X 300 -i my-httpd.pp#012
Nov 20 16:38:43 saloginov setroubleshoot[42516]: failed to retrieve rpm info for /var
/www/html/test.html
Nov 20 16:38:44 saloginov setroubleshoot[42516]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html. For complete SELinux messa
ges run: sealert -l c28c633b-bb5c-46dd-82f6-de9971a0f74a
Nov 20 16:38:44 saloginov setroubleshoot[42516]: SELinux is preventing /usr/sbin/http
d from getattr access on the file /var/www/html/test.html.#012#012***** Plugin resto
recon (92.2 confidence) suggests *****#012#012If you want to fix
the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#
012Then you can run restorecon. The access attempt may have been stopped due to insuf
ficient permissions to access a parent directory in which case try to change the foll
owing command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012
#012***** Plugin public_content (7.83 confidence) suggests *****#01
2#012If you want to treat test.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 confidence) suggests *****
*****#012#012If you believe that httpd should be allowed getattr access on
the test.html file by default.#012Then you should report this as a bug.#012You can g
enerate a local policy module to allow this access.#012Do#012allow this access for no
w by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodul
e -X 300 -i my-httpd.pp#012
[root@saloginov guest]#
```

16. При попытке запустить веб-сервер на прослушивание TCP-порта 81 было выявлено, что 81 порт уже присутствует в списке стандартных портов, которые невозможно удалить. Следовательно, пункты 16-20 не выполнены
21. Вернули контекст нашему файлу и через браузер получили доступ к нему
22. Файл отсутствует
23. Невозможно удалить



```
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]#
```

24. Удалили файл test.html

## Вывод

В ходе лабораторной работы были получены первые практические навыки работы с SELinux