

Лабораторная 6

Болотина А.С.

Цель работы

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

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status`. Если не работает, запустите его так же, но с параметром `start`.

```
[abolotina@asbolotina ~]$ 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>
   Drop-In: /etc/systemd/system/httpd.service.d
            └─nofile.conf
   Active: active (running) since Sat 2022-10-15 12:46:32 MSK; 2min 31s ago
     Docs: man:httpd.service(8)
 Main PID: 1352 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 5910)
  Memory: 12.1M
   CGroup: /system.slice/httpd.service
            └─1352 /usr/sbin/httpd -DFOREGROUND
               └─1376 /usr/sbin/httpd -DFOREGROUND
                  └─1377 /usr/sbin/httpd -DFOREGROUND
                     └─1378 /usr/sbin/httpd -DFOREGROUND
                        └─1379 /usr/sbin/httpd -DFOREGROUND

окт 15 12:46:26 asbolotina systemd[1]: Starting The Apache HTTP Server...
окт 15 12:46:32 asbolotina httpd[1352]: AH00558: httpd: Could not reliably dete>
окт 15 12:46:32 asbolotina systemd[1]: Started The Apache HTTP Server.
окт 15 12:46:32 asbolotina httpd[1352]: Server configured, listening on: port 80
lines 1-21/21 (END)...skipping...
```

Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого

проверьте, что контекст поменялся.

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

. Проанализируйте ситуацию. `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages`

```
[root@asbolotina html]# ls -Z f.html
unconfined_u:object_r:samba_share_t:s0 f.html
[root@asbolotina html]# ls -l f.html
-rw-r--r--. 1 root root 33 окт 15 20:48 f.html
[root@asbolotina html]# tail /var/log/messages
Oct 15 20:56:14 asbolotina sshd[6346]: @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Oct 15 20:56:14 asbolotina sshd[6346]: Permissions 0604 for '/etc/ssh/ssh_host_e
d25519_key' are too open.
Oct 15 20:56:14 asbolotina sshd[6346]: It is required that your private key file
s are NOT accessible by others.
Oct 15 20:56:14 asbolotina sshd[6346]: This private key will be ignored.
Oct 15 20:56:14 asbolotina sshd[6346]: Unable to load host key "/etc/ssh/ssh_hos
t_ed25519_key": bad permissions
Oct 15 20:56:14 asbolotina sshd[6346]: Unable to load host key: /etc/ssh/ssh_hos
t_ed25519_key
Oct 15 20:56:14 asbolotina sshd[6346]: sshd: no hostkeys available -- exiting.
Oct 15 20:56:14 asbolotina systemd[1]: sshd.service: Main process exited, code=e
xited, status=1/FAILURE
Oct 15 20:56:14 asbolotina systemd[1]: sshd.service: Failed with result 'exit-co
de'.
Oct 15 20:56:14 asbolotina systemd[1]: Failed to start OpenSSH server daemon.
```

Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.

```
[root@asbolotina html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@asbolotina html]# 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
```

Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и проверьте, что порт 81 удалён.

```
[root@asbolotina html]# semanage port -d -t http_port_t -p tcp 81
rmValueError: Порт tcp/81 определен на уровне политики и не может быть удален
```

```
[root@asbolotina html]# rm /var/www/html/f.html
rm: удалить обычный файл '/var/www/html/f.html'? y
[root@asbolotina html]# ls -l
```

Удалите файл /var/www/html/test.html: rm /var/www/html/test.html

```
итого 0
```

Выводы

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1.

Проверила работу SELinx на практике совместно с веб-сервером Apache.