

# Отчет по лабораторной работе № 6

## Основы информационной безопасности

---

Маметкадыров Ынтымак

Российский университет дружбы народов, Москва, Россия

НПМбд-02-20

## Цели лабораторной работы

- 1) Развить навыки администрирования ОС Linux
- 2) Получить первое практическое знакомство с технологией SELinux
- 3) Проверить работу SELinux на практике совместно с веб-сервером Apache.

## Задачи лабораторной работы

- 1) Проверить корректность работы SELinux, запустить веб-сервер Apache
- 2) Создать файл test.html
- 3) Обратиться к файлу через веб-сервер при разном контексте и порте

## Ход выполнения лабораторной работы

- Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”

```
[itmametskadihrov@itmametskadihrov ~]$ getenforce
Enforcing
[itmametskadihrov@itmametskadihrov ~]$ 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
[itmametskadihrov@itmametskadihrov ~]$
```

**Рис. 1:** Проверка режима enforcing политики targeted

# Ход выполнения лабораторной работы

- Обратились с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедились, что последний работает с помощью команды “service httpd status”

```
[itmametkadihrov@itmametkadihrov ~]$ 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; preset: disabled)
   Active: active (running) since Thu 2023-10-12 15:47:10 +06; 33s ago
     Docs: man:httpd.service(8)
  Main PID: 2954 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
      Tasks: 213 (limit: 25469)
    Memory: 41.4M
       CPU: 239ms
    CGroup: /system.slice/httpd.service
            └─2954 /usr/sbin/httpd -DFOREGROUND
              └─2980 /usr/sbin/httpd -DFOREGROUND
                └─2984 /usr/sbin/httpd -DFOREGROUND
                  └─2985 /usr/sbin/httpd -DFOREGROUND
                    └─2986 /usr/sbin/httpd -DFOREGROUND

окт 12 15:45:45 itmametkadihrov systemd[1]: Starting The Apache HTTP Server...
окт 12 15:46:26 itmametkadihrov httpd[2954]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, because the /etc/hosts file is missing.
окт 12 15:47:10 itmametkadihrov systemd[1]: Started The Apache HTTP Server.
окт 12 15:47:10 itmametkadihrov httpd[2954]: Server configured, listening on: port 80
```

Рис. 2: Проверка работы веб-сервера

# Ход выполнения лабораторной работы

- От имени суперпользователя создали файл test.html. Обратились к нему через веб-сервер, введя адрес “http://127.0.0.1/test.html”.

```
[itmanetkadirov@itmanetkadirov ~]$ su -  
itmanetkadirov:  
[root@itmanetkadirov ~]# touch /var/www/html/test.html  
[root@itmanetkadirov ~]# nano /var/www/html/test.html  
[root@itmanetkadirov ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@itmanetkadirov ~]# su - itmanetkadirov  
[itmanetkadirov@itmanetkadirov ~]$ ls -lZ /var/www/html  
иторо 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 13 18:11 test.html  
[itmanetkadirov@itmanetkadirov ~]$
```

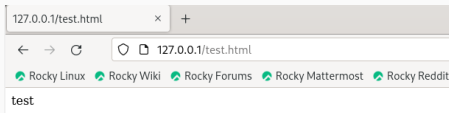


Рис. 3: Создание файла и его просмотр в веб-сервере

# Ход выполнения лабораторной работы

- Изменили контекст файла на `samba_share_t`. Попробовали получить доступ к файлу через веб-сервер и получили сообщение об ошибке

```
itnanetkadihrov@itnanetkadihrov ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
itnanetkadihrov@itnanetkadihrov ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Операция не позволена
itnanetkadihrov@itnanetkadihrov ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для itnanetkadihrov:
itnanetkadihrov@itnanetkadihrov ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
itnanetkadihrov@itnanetkadihrov ~]$
```



🔒 📄 127.0.0.1/test.html

Rocky Linux Rocky Wiki Rocky Forums Rocky Matt

## Forbidden

You don't have permission to access this resource.

**Рис. 4:** Изменение контекста и просмотр файла в веб-сервере

## Ход выполнения лабораторной работы

- В файле /etc/httpd/conf/httpd.conf заменили строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81

```
# directive.  
#  
# Change this to Listen on a specific IP address, but note that if  
# httpd.service is enabled to run at boot time, the address may not be  
# available when the service starts. See the httpd.service(8) man  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 81
```

**Рис. 5:** Установка веб-сервера Apache на прослушивание TCP-порта 81



## Ход выполнения лабораторной работы

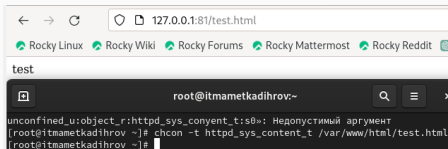
- Выполнили команду “semanage port -a -t http\_port\_t -p tcp 81” и убедились, что порт TCP-81 установлен. Проверили список доступных портов

```
[root@itmametskadihrov ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@itmametskadihrov ~]# 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@itmametskadihrov ~]# systemctl restart httpd
[root@itmametskadihrov ~]#
```

**Рис. 6:** Проверка установки порта 81

## Ход выполнения лабораторной работы

- Вернули контекст “httpd\_sys\_content\_t” файлу test.html и попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”



**Рис. 7:** Возвращение исходного контекста файлу и просмотр файла в веб-сервере

- В ходе выполнения данной лабораторной работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinux на практике совместно с веб-сервером Apache.