

Лабораторная работа No 6.

Тагиев Б. А.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

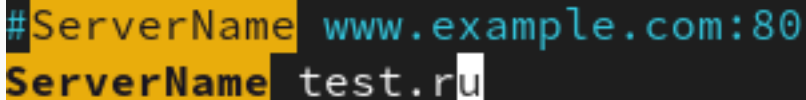
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

Выполнение лабораторной работы

1. Установить Apache2 при помощи dnf.

```
dnf install httpd
```

2. В конфигурационном файле httpd.conf прописать параметр ServerName.



```
#ServerName www.example.com:80
ServerName test.ru
```

The image shows a code editor with a dark background. Two lines of text are visible. The first line is a comment starting with a blue hash symbol, followed by 'ServerName' in white, and 'www.example.com:80' in blue. The second line is 'ServerName' in white, followed by 'test.ru' in white. The text 'ServerName' in both lines is highlighted with a yellow background.

Рис. 1: ServerName

3. Отключить пакетный фильтр при помощи `iptables`.

```
[root@batagiev httpd]# iptables -F
[root@batagiev httpd]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@batagiev httpd]# iptables -P INPUT ACCEPT && iptables -P OUTPUT ACCEPT
```

Рис. 2: iptables

1. Проверим правильность работы SELinux. Должен быть выставлен режим enforcing политики targeted.

```
[batagiev@batagiev ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
```

Рис. 3: sestatus

2. Запустим Apache веб-сервер.

```
[batagiev@batagiev ~]$ systemctl status httpd  
● httpd.service - The Apache HTTP Server
```

Рис. 4: httpd

3. В списке процессов найдем httpd.

```
[root@batagiev httpd]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 18702 0.0 0.2 20328 11664 ? Ss 19:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 18823 0.0 0.1 21664 7404 ? S 19:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 18826 0.0 0.4 2521332 19320 ? Sl 19:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 18827 0.0 0.2 2259124 11140 ? Sl 19:07 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 18828 0.0 0.2 2259124 11140 ? Sl 19:07 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40624 0.0 0.0 221664 2252 pts/0 S+ 19:11 0:00 grep --color=auto httpd
```

Рис. 5: Контекст безопасности

```
[root@batagiev httpd]# 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_manage_courier_spool 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_avaahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unityfd off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_opencryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
```

4. Посмотрим текущее состояние переключателей SELinux для Apache2.

5. Также посмотрим
текущую статистику по
политике.

```
[root@batagiev httpd]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

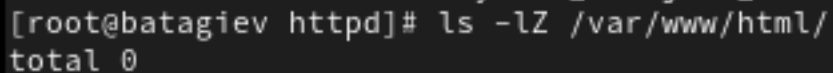
Classes:                  135      Permissions:              457
Sensitivities:            1        Categories:              1024
Types:                   5100     Attributes:               258
Users:                    8        Roles:                    14
Booleans:                 353      Cond. Expr.:             384
Allow:                    65000    Neverallow:              0
Auditallow:              170      Dontaudit:               8572
Type_trans:              265341    Type_change:             87
Type_member:              35       Range_trans:             6164
Role allow:               38       Role_trans:              420
Constraints:              70      Validatetrans:           0
MLS Constrain:            72      MLS Val. Tran:           0
Permissives:              2       Polcap:                  6
Defaults:                 7       Typebounds:              0
Allowxperm:               0       Neverallowxperm:         0
Auditallowxperm:         0       Dontauditxperm:          0
Ibendportcon:            0       Ibpkeycon:               0
Initial SIDs:             27      Fs_use:                  35
Genfscon:                 109     Portcon:                 660
Netifcon:                 0       Nodecon:                  0
```

6. Посмотрим текущий контекст безопасности для файлов и поддиректорий в директории `/var/www`.
 - Установлен контекст `httpd_sys_script_exec_t` для cgi-скриптов, чтобы был разрешен им доступ ко всем sys-типам.
 - Установлен контекст `httpd_sys_content_t` для содержимого, которое должно быть доступно для всех скриптов httpd и для самого демона.

```
[root@batagiev httpd]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
```

Рис. 8: Контекст безопасности

7. В директории `/var/www/html` пусто.



```
[root@batagiev httpd]# ls -lZ /var/www/html/  
total 0
```

Рис. 9: `/var/www/html`

8. В директории `/var/www/html` создавать папки может только root.

9. Создадим файл `/var/www/html/test.html`.

```
[root@batagiev httpd]# echo "<html>
<body>test</body>
</html>" >> /var/www/html/test.html
[root@batagiev httpd]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@batagiev httpd]#
```

Рис. 10: test.html

10. Проверим контекст созданного нами файла.

```
[root@batagiev httpd]# ls -lZ /var/www/html/  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 14 19:21 test.html
```

Рис. 11: test.html

11. Перейдем в браузер и в нем проверим доступность данного файла.

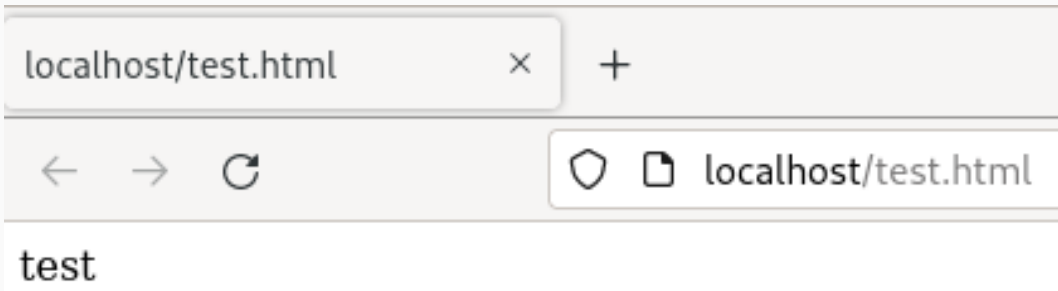


Рис. 12: Проверка

12. Изменим контекст файла, чтобы Apache не смог получить доступ.

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

Рис. 13: test.html

13. Проверим, что доступ к файлу стал не доступен.

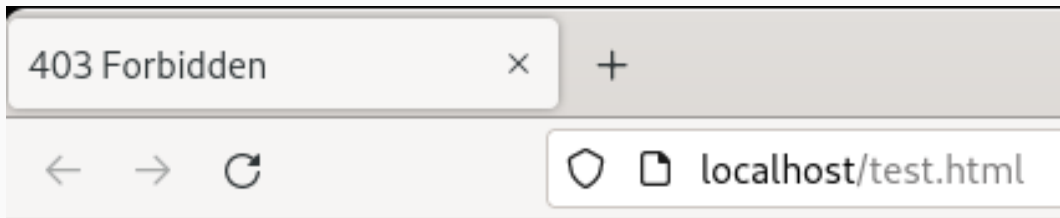
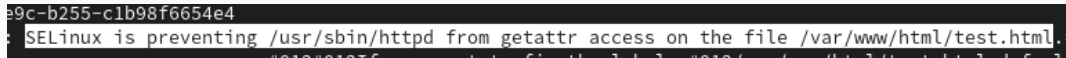


Рис. 14: Проверка

14. Посмотрим логи от веб-сервера Apache.



```
e9c-b255-c1b98f6654e4  
SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
```

Рис. 15: /var/log/messages

Также проверим audit.log.

```
[root@batagiev batagiev]# tail /var/log/audit/audit.log
type=SYSCALL msg=audit(1697300874.136:245): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f3c9c043a98 a2=7f3ca2ba68b0 a3=100 items=0 ppid=1870
2 pid=18828 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=
system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="
apache" SGID="apache" FSGID="apache"
```

Рис. 16: /var/log/audit/audit.log

15. Поменяем порт, на котором работает Apache.

A screenshot of a text editor showing the configuration of the Apache web server. The background is dark. The text is as follows: the first line is a comment starting with a blue hash symbol '#'; the second line is '#Listen 12.34.56.78:80' where 'Listen' is highlighted in yellow and the IP address and port are in cyan; the third line is 'Listen 81' where 'Listen' is highlighted in yellow and the port '81' is in white. This illustrates the process of changing the default listening port from 80 to 81.

```
#  
#Listen 12.34.56.78:80  
Listen 81
```

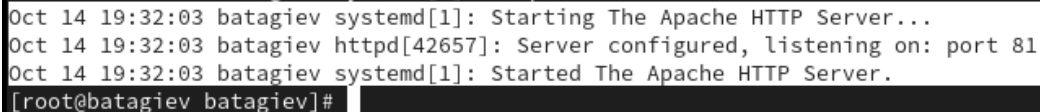
Рис. 17: Порт 81

16. Перезапустим веб-сервер.

```
[root@batagiev httpd]# systemctl restart httpd.service  
[root@batagiev httpd]# systemctl status httpd.service  
● httpd.service - The Apache HTTP Server
```

Рис. 18: Перезапуск

17. В логах наблюдаем запуск сервера на 81 порту.

A screenshot of a terminal window displaying system logs. The logs show the Apache HTTP Server being started by systemd, configured, and then started successfully. The prompt indicates the user is root on a machine named batagiev.

```
Oct 14 19:32:03 batagiev systemd[1]: Starting The Apache HTTP Server...  
Oct 14 19:32:03 batagiev httpd[42657]: Server configured, listening on: port 81  
Oct 14 19:32:03 batagiev systemd[1]: Started The Apache HTTP Server.  
[root@batagiev batagiev]#
```

Рис. 19: /var/log/messages

18. Добавим порт в `semanage` для `http_port_t` и проверим его добавление

```
[root@batagiev httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@batagiev httpd]#
```

Рис. 20: Добавление

```
[root@batagiev httpd]# 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
```

Рис. 21: Проверка

19. Ввернем контекст файлу `test.html`.
20. Удалим привязку порта.
21. Удалим файл `test.html`.

В результате выполнения работы я выполнил цели работы.