Лабораторная работа № 6

Дугаева Светлана Анатольевна, НФИбд-01-18

Цель работы

Цель работы

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

Выполнение лабораторной работы

Выполнение лабораторной работы

```
[dugaevas@localhost ~]$ su
Пароль:
[root@localhost dugaevas]# echo "ServerName test.ru" >> /etc/httpd/httpd.conf
[root@localhost dugaevas]# cat /etc/httpd/httpd.conf
ServerName test.ru
[root@localhost dugaevas]# iptables -F
[root@localhost dugaevas]# iptables -P INPUT ACCEPT
[root@localhost dugaevas]# iptables -P OUTPUT ACCEPT
[root@localhost dugaevas]# EXIT
bash: EXIT: команда не найдена...
[root@localhost dugaevas]# exit
exit
[dugaevas@localhost ~]$ getrnforce
bash: getrnforce: команда не найдена...
[dugaevas@localhost ~]$ getenforce
Enforcing
[dugaevas@localhost ~]$ 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
[dugaevas@localhost ~]$
```

Выполнение лабораторной работы

```
[dugaevas@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-11-25 15:21:43 EST; 1h 23min ago
     Docs: man:httpd.service(8)
 Main PID: 12667 (httpd)
   Status: "Total requests: 3; Idle/Busy workers 100/0;Requests/sec: 0.000598; Bytes served/sec:   0 B/sec"
    Tasks: 214 (limit: 4808)
   Memory: 11.5M
   CGroup: /system.slice/httpd.service
           ├─12667 /usr/sbin/httpd -DFOREGROUND
           ├─12672 /usr/sbin/httpd -DFOREGROUND
           ├─12673 /usr/sbin/httpd -DFOREGROUND
           ├─12674 /usr/sbin/httpd -DFOREGROUND
           ├─12675 /usr/sbin/httpd -DFOREGROUND
           └─12676 /usr/sbin/httpd -DFOREGROUND
[dugaevas@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      12667 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12672 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12673 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      12674 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      12675 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0      12676 ?        00:00:01 httpd
[dugaevas@localhost ~]$
```

Рис. 2: Статус веб-сервера и политика безопасности

Выполнение лабораторной работы

```
[dugaevas@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0       12667 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0       12672 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0       12673 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0       12674 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0       12675 ?        00:00:01 httpd
system_u:system_r:httpd_t:s0       12676 ?        00:00:01 httpd
[dugaevas@localhost ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
cluster_can_network_connect                 off
cluster_manage_all_files                    off
```

Выполнение лабораторной работы

```
[dugaevas@localhost ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             31 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             132    Permissions:         464
  Sensitivities:         1    Categories:         1024
  Types:              4961    Attributes:          255
  Users:                 8    Roles:                14
  Booleans:            338    Cond. Expr.:         386
  Allow:            112594    Neverallow:            0
  Auditallow:          166    Dontaudit:         10358
  Type_trans:       252747    Type_change:          87
  Type_member:          35    Range_trans:        5781
  Role allow:           38    Role_trans:          421
  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    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               34
  Genfscon:            107    Portcon:             642
  Netifcon:              0    Nodecon:               0
[dugaevas@localhost ~]$ ls -lZ /vat/www
ls: невозможно получить доступ к '/vat/www': Нет такого файла или каталога
[dugaevas@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0  6 ноя 11 23:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     26 ноя 25 16:22 html
[dugaevas@localhost ~]$ ls -lZ /var/www/html
итого 0
[dugaevas@localhost ~]$ ls -l /var/www/html
```

Выполнение лабораторной работы

```
[root@localhost dugaevas]# nano /var/www/html/test.html
[root@localhost dugaevas]# cat /var/www/html/test.html
<html>
        <body>test</body>
</html>
[root@localhost dugaevas]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 25 17:11 /var/www/html/test.html
[root@localhost dugaevas]#
```

Рис. 5: Создание файла test.html и его контекст

Выполнение лабораторной работы

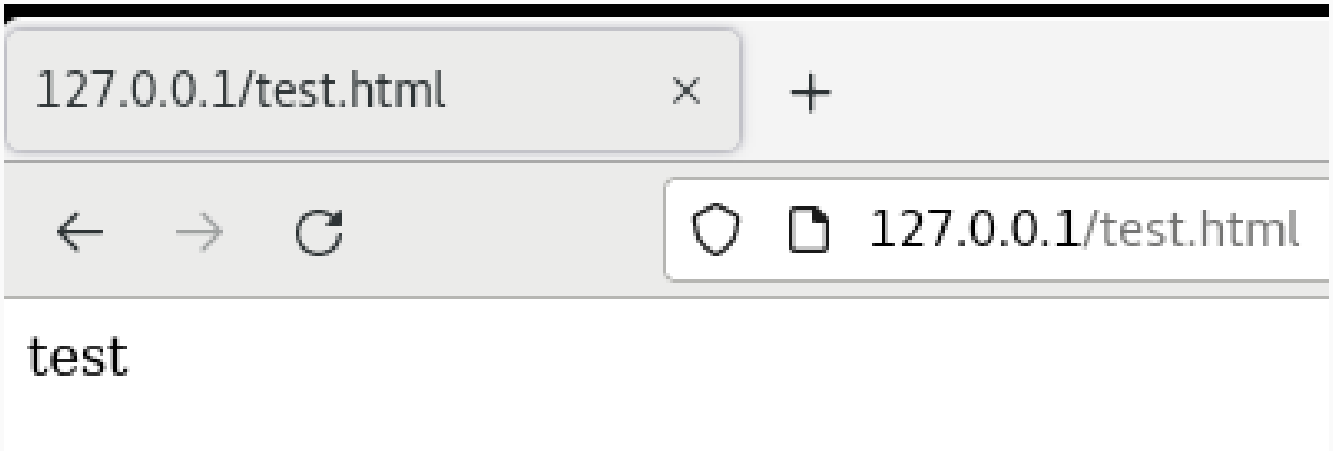

Рис. 6: Обращение к файлу через веб-сервер

Выполнение лабораторной работы

```
httpd_selinux(8)                    httpd Selinux Policy documentation                    httpd_selinux(8)

НАЗВАНИЕ
       httpd_selinux - Политика Security Enhanced Linux для демона httpd

ОПИСАНИЕ
       Security-Enhanced  Linux  обеспечивает  защиту  сервера  httpd  при помощи гибко настраиваемого мандатного контроля
       доступа.

КОНТЕКСТ ФАЙЛОВ
       SELinux требует наличия у файлов расширенных атрибутов, определяющих тип файла.  Политика управляет  видом  доступа
       демона  к  этим файлам.  Политика SELinux для демона httpd позволяет пользователям настроить web-службы максимально
       безопасным методом с высокой степенью гибкости.

       Для httpd определены следующие контексты файлов:
       httpd_sys_content_t
       - Установите контекст httpd_sys_content_t для содержимого, которое должно быть доступно для всех скриптов  httpd  и
       для самого демона.
       httpd_sys_script_exec_t
       - Установите контекст httpd_sys_script_exec_t для cgi-скриптов, чтобы разрешить им доступ ко всем sys-типам.
       httpd_sys_script_ro_t
       -  Установите  на  файлы контекст httpd_sys_script_ro_t если вы хотите, чтобы скрипты httpd_sys_script_exec_t могли
       читать данные, и при этом нужно запретить доступ другим не-sys скриптам.
       httpd_sys_script_rw_t
       - Установите на файлы контекст httpd_sys_script_rw_t если вы хотите, чтобы  скрипты  httpd_sys_script_exec_t  могли
       читать и писать данные, и при этом нужно запретить доступ другим не-sys скриптам.
       httpd_sys_script_ra_t
       -  Установите  на  файлы контекст httpd_sys_script_ra_t если вы хотите, чтобы скрипты httpd_sys_script_exec_t могли
       читать и добавлять данные, и при этом нужно запретить доступ другим не-sys скриптам.
       httpd_unconfined_script_exec_t
       - Установите на cgi-скрипты контекст httpd_unconfined_script_exec_t если вы хотите  разрешить  им  исполняться  без
       какой-либо  защиты  SELinux.  Такой  способ  должен  использоваться  только  для  скриптов  с  очень  комплексными
       требованиями, и только в случае, если все остальные варианты  настройки  не  дали  результата.  Лучше  использовать
       скрипты с контекстом httpd_unconfined_script_exec_t, чем выключать защиту SELinux для httpd.
```

Рис. 7: Справка о контекстах

Выполнение лабораторной работы

```
[root@localhost dugaevas]# man httpd_selinux
[root@localhost dugaevas]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost dugaevas]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost dugaevas]#
```

Рис. 8: Изменение контекста

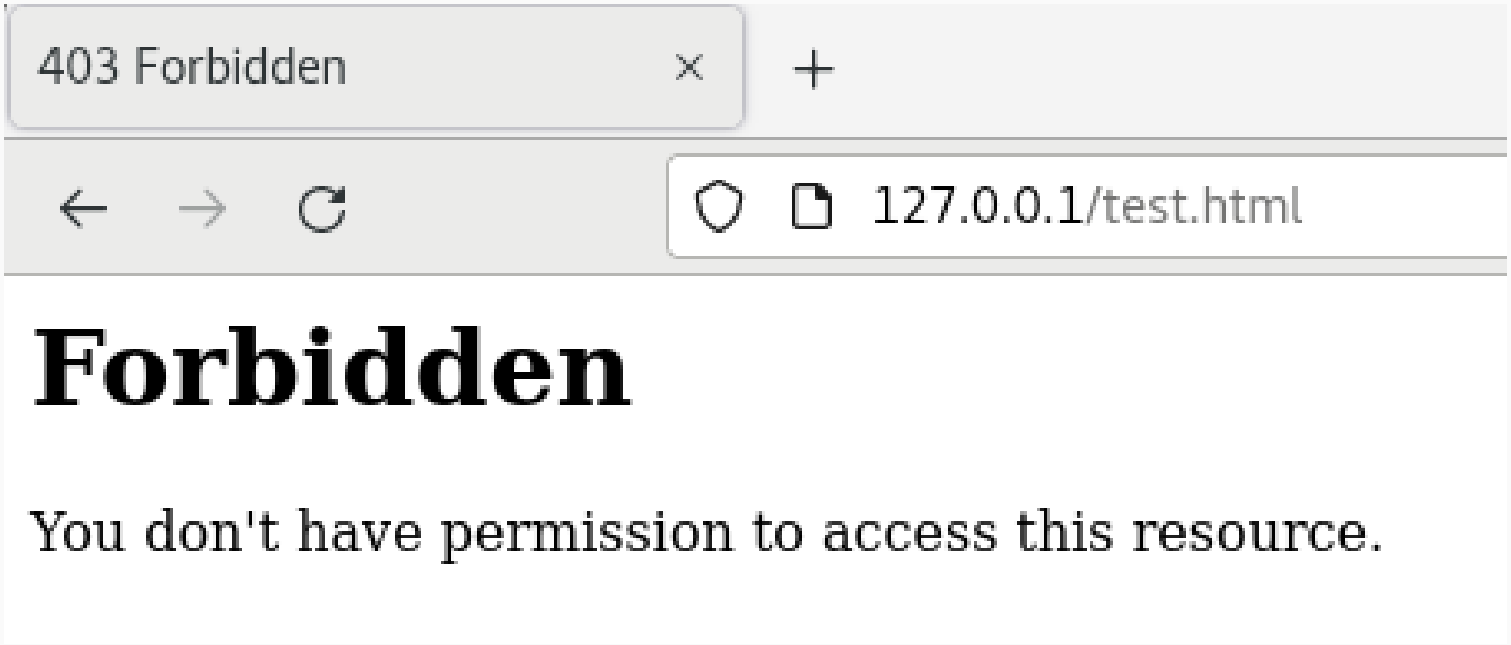

Рис. 9: Доступ к файлу через веб-браузер

Выполнение лабораторной работы

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 10: Смена порта

Выполнение лабораторной работы

```
[root@localhost dugaevas]# nano /etc/httpd/httpd.conf
[root@localhost dugaevas]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevas]# nano /etc/httpd/conf/httpd.conf
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xe" for details.
[root@localhost dugaevas]#
```

Рис. 11: Перезапуск веб-сервера

Выполнение лабораторной работы

```
[root@localhost dugaevas]# semanage port -a -t http_port_t -p tcp 82
[root@localhost dugaevas]# semanage port -l | grep http_port_t
http_port_t                    tcp      82, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
[root@localhost dugaevas]# servise httpd restart
bash: servise: команда не найдена...
Аналогичная команда: 'service'
[root@localhost dugaevas]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost dugaevas]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис. 12: Пункты 19-21

Выполнение лабораторной работы

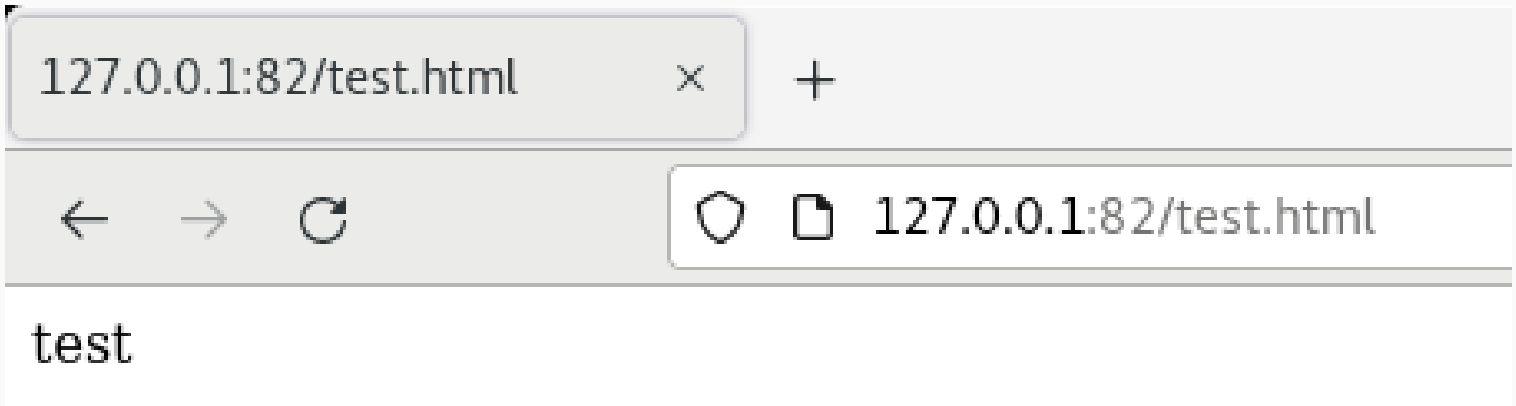

Рис. 13: Доступ к файлу через веб-браузер

Выполнение лабораторной работы

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Рис. 14: Конфиг. файл в первоначальное состояние

Выполнение лабораторной работы

```
[root@localhost dugaevas]# semanage port -a -t http_port_t -p tcp 80
ValueError: Порт tcp/80 уже определен
[root@localhost dugaevas]# semanage port -d -t http_port_t -p tcp 82
[root@localhost dugaevas]# 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@localhost dugaevas]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@localhost dugaevas]#
```

Рис. 15: Удаление привязки к порту 82 и файла test.html

Выводы

Выводы

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.