

Отчет по лабораторной работе № 6

По дисциплине Информационная безопасность

Выполнил: Максимов Алексей Александрович

Группа: НПИ-бд-01-20

Российский Университет Дружбы Народов #### г. Москва

Цель работы

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

Ход работы

Выполнение лабораторной работы

Подготовка лабораторного стенда и методические рекомендации

```
root@localhost:~# vi /etc/httpd/conf/httpd.conf
httpd.conf [----] 18 L:[ 83+12 95/354] *(3567/
# e-mailed. This address appears on some server-genera
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server us
# This can often be determined automatically, but we re
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, ente
#
ServerName test.ru
#
# Deny access to the entirety of your server's filesystem
```

```
[root@aamaksimov ~]# mc
[root@aamaksimov conf]# iptables -F
[root@aamaksimov conf]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@aamaksimov conf]# iptables -p INPUT ACCEPT iptables -P OUTPUT ACCEPT
iptables v1.4.21: unknown protocol "input" specified
Try `iptables -h' or 'iptables --help' for more information.
[root@aamaksimov conf]# iptables -P INPUT ACCEPT
[root@aamaksimov conf]# iptables -P OUTPUT ACCEPT
[root@aamaksimov conf]#
```

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted

```
[root@aamaksimov conf]# getenforce
Enforcing
[root@aamaksimov conf]# 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
Max kernel policy version:      31
[root@aamaksimov conf]# 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 Пн 2023-10-02 14:18:41 MSK; 28s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3702 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
            └─3702 /usr/sbin/httpd -DFOREGROUND
              └─3706 /usr/sbin/httpd -DFOREGROUND
                └─3707 /usr/sbin/httpd -DFOREGROUND
                  └─3708 /usr/sbin/httpd -DFOREGROUND
                    └─3709 /usr/sbin/httpd -DFOREGROUND
                      └─3710 /usr/sbin/httpd -DFOREGROUND

окт 02 14:18:41 aamaksimov.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 02 14:18:41 aamaksimov.localdomain systemd[1]: Started The Apache HTTP Server.
[root@aamaksimov conf]#
```

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт.

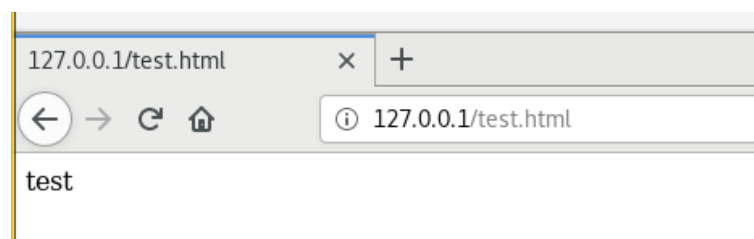
```
[root@aamaksimov aamaksimov]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3702  0.0  0.2 224088  5016 ?        Ss   14:18   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3706  0.0  0.1 226172  3100 ?        S    14:18   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3707  0.0  0.1 226172  3100 ?        S    14:18   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3708  0.0  0.1 226172  3100 ?        S    14:18   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3709  0.0  0.1 226172  3100 ?        S    14:18   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3710  0.0  0.1 226172  3100 ?        S    14:18   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3792  0.0  0.0 112832  964 pts/1 R+   14:21   0:00 grep --color=auto httpd

[root@aamaksimov aamaksimov]# 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
Max kernel policy version:    31

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
cluster_use_execmem             off
cobbler_anon_write              off
cobbler_can_network_connect     off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect    off
condor_tcp_network_connect      off
```

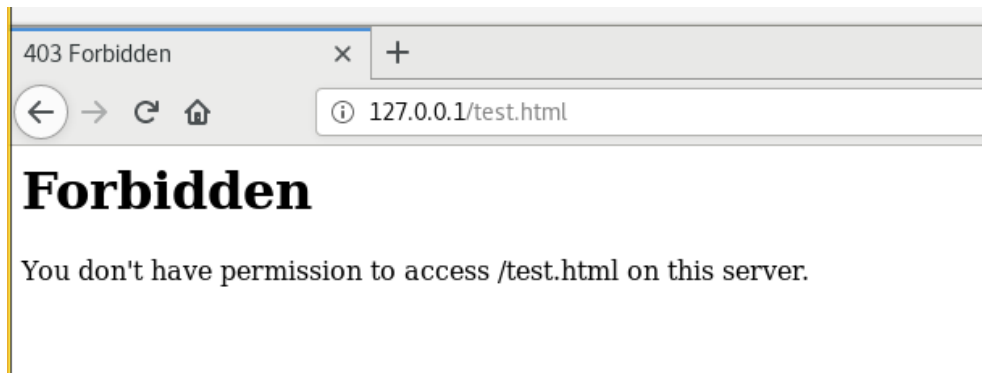
Определите тип файлов и поддиректорий, находящихся в директории /var/www. Создайте от имени суперпользователя html-файл /var/www/html/test.html

```
[root@aamaksimov aamaksimov]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@aamaksimov aamaksimov]# ls -lZ /var/www/html
[root@aamaksimov aamaksimov]#
[root@aamaksimov html]# touch test.html
[root@aamaksimov html]# echo <html>
bash: syntax error near unexpected token `newline'
[root@aamaksimov html]# <body>test</body>
bash: syntax error near unexpected token `newline'
[root@aamaksimov html]# ls -l /etc/*.conf/var/www/html
ls: невозможно получить доступ к /etc/*.conf/var/www/html: Нет такого файла или каталога
[root@aamaksimov html]# ls -l /var/www/html
итого 4
-rw-r--r--. 1 root root 32 окт  2 14:36 test.html
[root@aamaksimov html]#
```



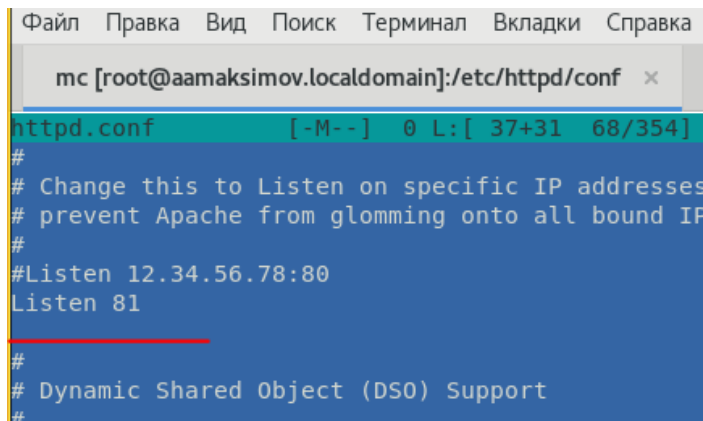
Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой и проверьте лог-файлы веб-сервера

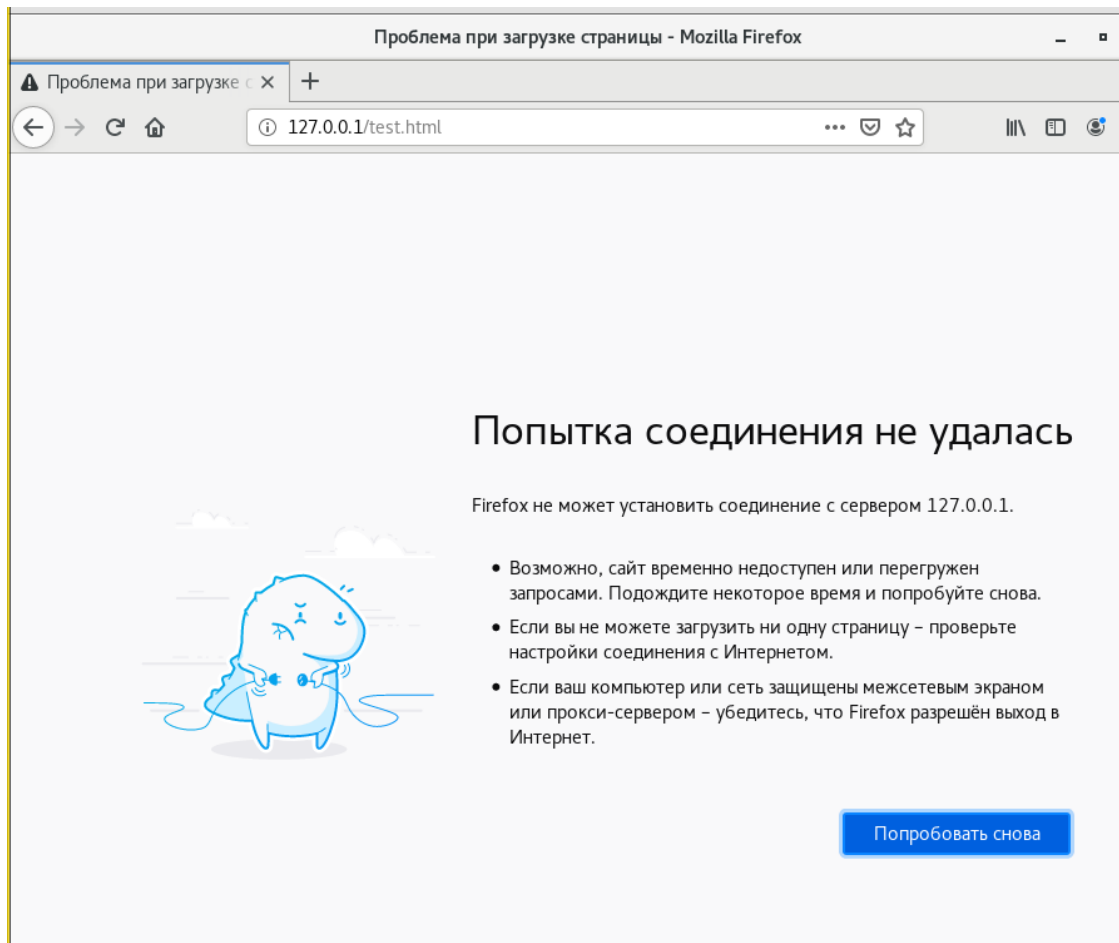
```
[root@aamaksimov html]# ls -l /var/www/html
итого 4
-rw-r--r--. 1 root root 32 окт  2 14:36 test.html
[root@aamaksimov html]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@aamaksimov html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@aamaksimov html]# chcon -t samba_share_t /var/www/html/test.html
[root@aamaksimov html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@aamaksimov html]#
```



```
[root@aamaksimov html]# tail /var/log/messages
dct 2 14:30:01 aamaksimov systemd: Started Session 7 of user root.
dct 2 14:40:01 aamaksimov systemd: Started Session 8 of user root.
dct 2 14:43:41 aamaksimov dbus[714]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
dct 2 14:43:42 aamaksimov dbus[714]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
dct 2 14:43:43 aamaksimov setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
dct 2 14:43:43 aamaksimov setroubleshoot: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l bab7d53-8104-4571-9034-1bf402c34513
dct 2 14:43:43 aamaksimov python: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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 insufficient per
missions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) s
uggests *****#012#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 fcontext -
s -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 generate a local policy module to allow this access.#012Do#012#allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
dct 2 14:43:46 aamaksimov setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
dct 2 14:43:46 aamaksimov setroubleshoot: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l bab7d53-8104-4571-9034-1bf402c34513
dct 2 14:43:46 aamaksimov python: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (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 insufficient per
missions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) s
uggests *****#012#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 fcontext -
s -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 generate a local policy module to allow this access.#012Do#012#allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
[root@aamaksimov html]#
```

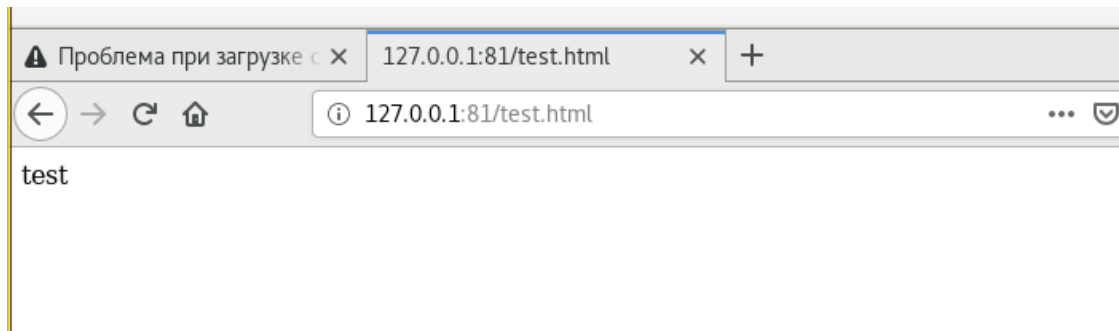
Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81





```
[root@aamaksimov html]#
[root@aamaksimov conf]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolen,permissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@aamaksimov conf]# 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@aamaksimov conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@aamaksimov conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@aamaksimov conf]#
[root@aamaksimov conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@aamaksimov conf]# sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@aamaksimov conf]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@aamaksimov conf]#
```

Верните контекст `httpd_sys_content__t` к файлу `/var/www/html/test.html` и исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`. Удалите файл `/var/www/html/test.html`:



Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache