

Лабораторная работа №6

Основы Информационной Безопасности

Дьяконова Софья Александровна

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы.....	2
Выводы	7

Цель работы

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

Задание

1. Подготовить рабочую среду;
2. Выполнить основную часть работы;
3. Сделать выводы.

Теоретическое введение

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим включены, особенно когда работа будет проводиться повторно и велика вероятность изменений при предыдущем использовании системы.
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл /etc/selinux/config, так и проверить используемый режим и политику.

3. Необходимо, чтобы был установлен веб-сервер Apache. При установке системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр `ServerName: ServerName test.ru`, чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.
5. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключить фильтр можно командами
`iptables -F`
`iptables -P INPUT ACCEPT`
`iptables -P OUTPUT ACCEPT`
либо добавить разрешающие правила:
`iptables -I INPUT -p tcp -dport 80 -j ACCEPT`
`iptables -I INPUT -p tcp -dport 81 -j ACCEPT`
`iptables -I OUTPUT -p tcp -sport 80 -j ACCEPT`
`iptables -I OUTPUT -p tcp -sport 81 -j ACCEPT`
6. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
7. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

Выполнение лабораторной работы

Вошла в систему с и убедилась, что SELinux работает в режиме `enforcing` политики `targeted` с помощью команд **`getenforce`** и **`sestatus`** (рис. [-@fig:001]).

```
[sadyakonova@localhost ~]$ getenforce
Enforcing
[sadyakonova@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
```

Проверка работы SELinux

Чтобы работать с библиотекой `httpd`, скачала ее.

Убедилась, что веб-сервер работает при помощи утилиты **service httpd start** (рис. [-@fig:002]).

```
[sadyakonova@localhost ~]$ sudo systemctl start httpd
[sadyakonova@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[sadyakonova@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; enabled; preset: disabled)
   Active: active (running) since Sat 2024-04-27 11:16:58 MSK; 57s ago
     Docs: man:httpd.service(8)
  Main PID: 6732 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes"
      Tasks: 213 (limit: 10975)
    Memory: 25.5M
      CPU: 581ms
    CGroup: /system.slice/httpd.service
            └─6732 /usr/sbin/httpd -DFOREGROUND
              └─6733 /usr/sbin/httpd -DFOREGROUND
                └─6734 /usr/sbin/httpd -DFOREGROUND
                  └─6735 /usr/sbin/httpd -DFOREGROUND
                    └─6736 /usr/sbin/httpd -DFOREGROUND
...skipping...
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-04-27 11:16:58 MSK; 57s ago
     Docs: man:httpd.service(8)
  Main PID: 6732 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes"
      Tasks: 213 (limit: 10975)
    Memory: 25.5M
      CPU: 581ms
    CGroup: /system.slice/httpd.service
            └─6732 /usr/sbin/httpd -DFOREGROUND
              └─6733 /usr/sbin/httpd -DFOREGROUND
                └─6734 /usr/sbin/httpd -DFOREGROUND
                  └─6735 /usr/sbin/httpd -DFOREGROUND
                    └─6736 /usr/sbin/httpd -DFOREGROUND
```

Проверка работы

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd** (рис. [-@fig:003]), (рис. [-@fig:004]).

```
[sadyakonova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 6732 0.0 0.6 20128 11488 ? Ss 11:16 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6733 0.0 0.4 21612 7480 ? S 11:16 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6734 0.2 0.7 2455704 13096 ? Sl 11:16 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6735 0.2 0.7 2324568 13096 ? Sl 11:16 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6736 0.2 0.6 2259032 11008 ? Sl 11:16 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 sadyako+ 7019 0.0 0.1 221688 2500 pts/0 R+ 11:19 0:00 grep --color=auto httpd
```

Состояние переключателей

```
[sadyakonova@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
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
colord_use_nfs                   off
condor_tcp_network_connect       off
```

Состояние переключателей

Посмотрела статистику по политике с помощью команды seinfo. Типы: 5135; пользователи: 8; роли: 15 (рис. [-@fig:005]).

```
[root@localhost sadyakonova]# 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:                          5135     Attributes:                     259
Users:                           8        Roles:                          15
Booleans:                       357     Cond. Expr.:                   390
Allow:                          65409    Neverallow:                     0
Auditallow:                     172     Dontaudit:                     8647
Type_trans:                     267813   Type_change:                     94
Type_member:                     37     Range_trans:                   6164
Role allow:                      39     Role_trans:                     419
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:                       665
Netifcon:                       0      Nodecon:                       0

[root@localhost sadyakonova]#
```

Статистика

Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www** (папки). Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (суперпользователю) (рис. [-@fig:006]).

```
[root@localhost sadyakonova]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 12:35 html
[root@localhost sadyakonova]# ls -lZ /var/www/html
итого 0
```

Тип файлов, круг пользователей

Создала html-файл /var/www/html/test.html (рис. [-@fig:007]).

```
[sadyakonova@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo nano /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

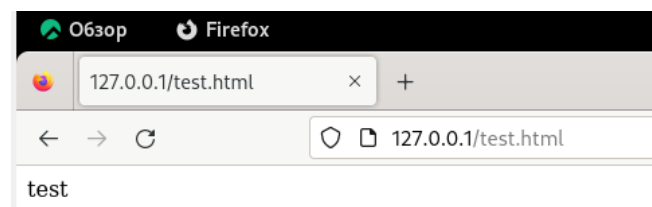
Файл

Проверила контекст созданного файла (httpd_sys_content_t) (рис. [-@fig:008]).

```
[sadyakonova@localhost ~]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 анп 27 11:26 test.html
```

Контекст файла

Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Файл был успешно отображён (рис. [-@fig:009]).



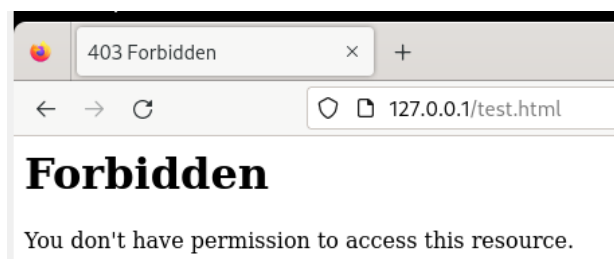
Состояние переключателей

Тип httpd_sys_content_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. Изменила контекст файла /var/www/html/test.html с **httpd_sys_content_t** на **samba_share_t** с помощью утилиты **chcon -t samba_share_t /var/www/html/test.html**. Контекст поменялся (рис. [-@fig:010]).

```
[sadyakonova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для sadyakonova:
[sadyakonova@localhost ~]$ sudo ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 апр 27 11:26 /var/www/html/test.html
```

Изменение контекста

Попробовала ещё раз получить доступ к файлу через веб-сервер. Ошибка :(((рис. [-@fig:011]).



Отказ в доступе

Проанализировала ситуацию. Файл не отображается, так как этот тип не позволяет процессу httpd получить доступ к файлу. Также просмотрела системный лог-файл tail /var/log/messages (рис. [-@fig:012]).

```
[sadyakonova@localhost ~]$ sudo tail /var/log/audit/audit.log
type=USER_ACCT msg=audit(1714206941.187:384): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accon
ting grantors=pam_unix,pam_localuser acct="sadyakonova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyako
na"
type=USER_CMD msg=audit(1714206941.187:385): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/sa
dyakonova" cmd=6C73202D6C202F7661722F777772F6874606C2F746573742E6874606C exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=CRED_REFR msg=audit(1714206941.198:386): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_START msg=audit(1714206941.275:387): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sess
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonov
a" AUID="sadyakonova"
type=USER_END msg=audit(1714206941.291:388): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sessio
n_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonov
a" AUID="sadyakonova"
type=CRED_DISP msg=audit(1714206941.291:389): pid=8389 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_ACCT msg=audit(1714207058.117:390): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accon
ting grantors=pam_unix,pam_localuser acct="sadyakonova" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyako
na"
type=USER_CMD msg=audit(1714207058.117:391): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/sa
dyakonova" cmd=7461696C202F7661722F766C6F72F61756469742F2F61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=CRED_REFR msg=audit(1714207058.138:392): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcr
grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonova" AUID="sadyakonova"
type=USER_START msg=audit(1714207058.195:393): pid=8408 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:sess
n_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="sadyakonov
a" AUID="sadyakonova"
```

Лог-файл

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf поменяла строчку Listen 80 на Listen 81.

Выполнила перезапуск веб-сервера Apache. Сбой не произошел.... Проанализировала лог-файлы tail -nl /var/log/messages, /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. [-@fig:013]).

```
[sadyakonova@localhost ~]$ sudo tail -n1 /var/log/messages
Apr 27 11:35:06 localhost systemd[5005]: app-gnome-firefox-8013.scope: Consumed 1min 19.195s CPU time.
[sadyakonova@localhost ~]$ sudo cat /var/log/httpd/error_log
[Sat Apr 27 11:16:58.443662 2024] [core:notice] [pid 6732:tid 6732] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Apr 27 11:16:58.451980 2024] [suexec:notice] [pid 6732:tid 6732] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
[Sat Apr 27 11:16:58.471323 2024] [lbmethod_heartbeat:notice] [pid 6732:tid 6732] AH02282: No slotmem from mod_heartbeat
[Sat Apr 27 11:16:58.477758 2024] [mpm_event:notice] [pid 6732:tid 6732] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Apr 27 11:16:58.477805 2024] [core:notice] [pid 6732:tid 6732] AH00994: Command Line: '/usr/sbin/httpd -D FOREGROUND'
```

Перезапуск сервера

Выполнила команду **semanage port -a -t http_port_t -p tcp 81**, проверила список портов командой **semanage port -l | grep http_port_t** (рис. [-@fig:014]).

Вернула контекст **httpd_sys_content_t** к файлу **/var/www/html/ test.html**. После этого попробовала получить доступ к файлу через веб-сервер (рис. [-@fig:014]).

Исправила обратно конфигурационный файл **apache**, вернув **Listen 80**. Удалила привязку **http_port_t** к **81** порту, но появилась ошибка, что этот порт удалить невозможно, даже через суперпользователя.

Удалила файл **/var/www/html/test.html** (рис. [-@fig:014]).

```
[sadyakonova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[sadyakonova@localhost ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[sadyakonova@localhost ~]$ sudo 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
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo chcon -t http_sys_content_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:http_sys_content_t:s0»: Недопустимый аргумент
[sadyakonova@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sadyakonova@localhost ~]$ sudo systemctl restart httpd
[sadyakonova@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
[sadyakonova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[sadyakonova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[sadyakonova@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 апр 27 11:26 test.html
[sadyakonova@localhost ~]$ rm /var/www/html/test.html
rm: удалить защищённый от записи обычный файл '/var/www/html/test.html'? y
rm: невозможно удалить '/var/www/html/test.html': Отказано в доступе
[sadyakonova@localhost ~]$ sudo rm /var/www/html/test.html
[sadyakonova@localhost ~]$ ls -lZ /var/www/html
итого 0
```

Конец)

Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux.