Защита лабораторной работы №6. Мандатное разграничение прав в Linux

Бурдина Ксения Павловна

2022 Oct 11th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №6

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

Развитие навыков администрирования ОС Linux, получение практического знакомства с технологией SELinux, а также проверка работы SELinux на практике совместно с веб-сервером Apache.

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Настройка каталога httpd для работы: проверка наличия необходимых файлов, настройка фильтров:

```
[root@10 ~]# cd /etc/httpd
[root@10 httpd]# ls
conf  conf.d  conf.modules.d  logs  modules  run  state
[root@10 httpd]# cd conf
[root@10 conf]# cat httpd.conf
ServerName test.ru
[root@10 conf]# cd
[root@10 ~]# iptables -F
[root@10 ~]# iptables -P INPUT ACCEPT
[root@10 ~]# iptables -P OUTPUT ACCEPT
```

Figure 1: Подготовка к работе

Результат выполнения лабораторной работы

Проверка, что SELinux работает в режиме enforcing политики targeted:

```
[root@10 kpburdina]# getenforce
Enforcing
[root@10 kpburdina]# 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
```

Figure 2: Вызов команд getenforce и sestatus

Результат выполнения лабораторной работы

Проверка работы веб-сервера:

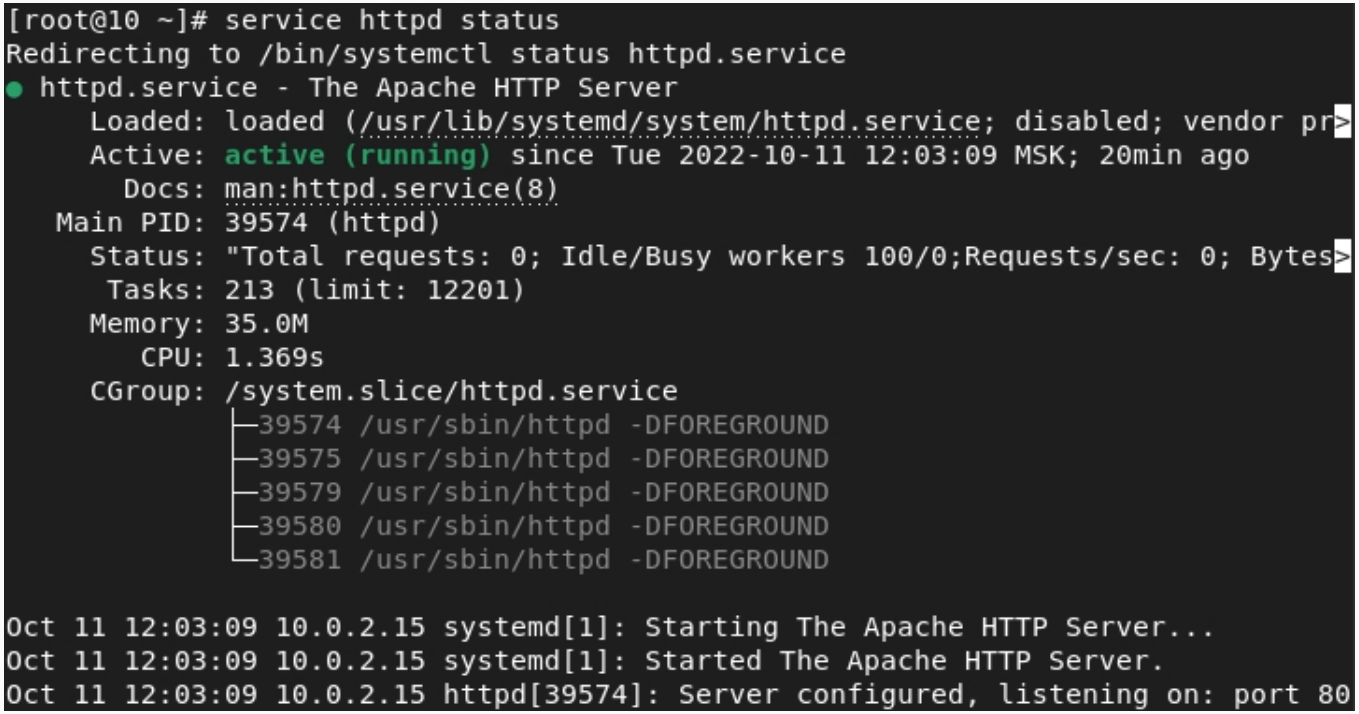

Figure 3: Обращение к веб-серверу

Результат выполнения лабораторной работы

Нахождение веб-сервера Apache в списке процессов:

```
[root@10 ~]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 12526 0.0  0.4 235988
 8936 pts/0 T 12:01   0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0    root       39574  0.0  0.5  20064 11632 ?
 Ss   12:03   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39575  0.0  0.3  21516  7276 ?
 S    12:03   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39579  0.0  0.8 1210352 17096 ?
 Sl   12:03   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39580  0.0  0.7 1079216 15048 ?
 Sl   12:03   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39581  0.0  0.7 1079216 15048 ?
 Sl   12:03   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40000 0.0  0.4 235988
 9208 pts/0 T 12:13   0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40083 0.0  0.4 235988
 9108 pts/0 T 12:17   0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40219 0.0  0.1 221800
 2264 pts/0 S+ 12:26   0:00 grep --color=auto httpd
```

Figure 4: Нахождение Apache в списке процессоров

Результат выполнения лабораторной работы

Просмотр текущего состояния переключателей SELinux для Apache:

```
[root@10 ~]# 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_avahi                             off
httpd_dbus_sssd                              off
httpd_dontaudit_search_dirs                  off
httpd_enable_cgi                             on
httpd_enable_ftp_server                      off
httpd_enable_homedirs                        off
```

Figure 5: Состояние переключателей SELinux

Результат выполнения лабораторной работы

Посмотр статистики по политике с помощью команды seinfo:

```
[root@10 ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             133    Permissions:         454
  Sensitivities:         1    Categories:         1024
  Types:              5002    Attributes:          254
  Users:                 8    Roles:                14
  Booleans:            347    Cond. Expr.:         381
  Allow:             63996    Neverallow:            0
  Auditallow:          168    Dontaudit:          8417
  Type_trans:       258486    Type_change:          87
  Type_member:          35    Range_trans:        5960
  Role allow:           38    Role_trans:          420
  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:               33
  Genfscon:            106    Portcon:             651
  Netifcon:              0    Nodecon:               0
```

Figure 6: Статистика по политике

Результат выполнения лабораторной работы

Определение типа файлов и поддиректорий, находящихся в директории /var/www:

```
[root@10 ~]# 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
```

Figure 7: Просмотр директории /var/www

Результат выполнения лабораторной работы

Создание файла test.html:

```
[root@10 ~]# touch /var/www/html/test.html
```

Figure 8: Создание файла test.html

```
<html>
<body>
test
</body>
</html>
```

Figure 9: Листинг файла

Результат выполнения лабораторной работы

Проверка контекста созданного файла:

```
[root@10 html]# cat test.html
<html>
<body>
test
</body>
</html>
```

Figure 10: Чтение содержимого файла

Просмотр контекста, присваиваемого по умолчанию вновь созданным файлам в директории /var/www/html:

```
[root@10 html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Figure 11: Контекст созаваемых файлов

Результат выполнения лабораторной работы

Обращение к файлу через веб-браузер по адресу http://127.0.0.1/test.html:

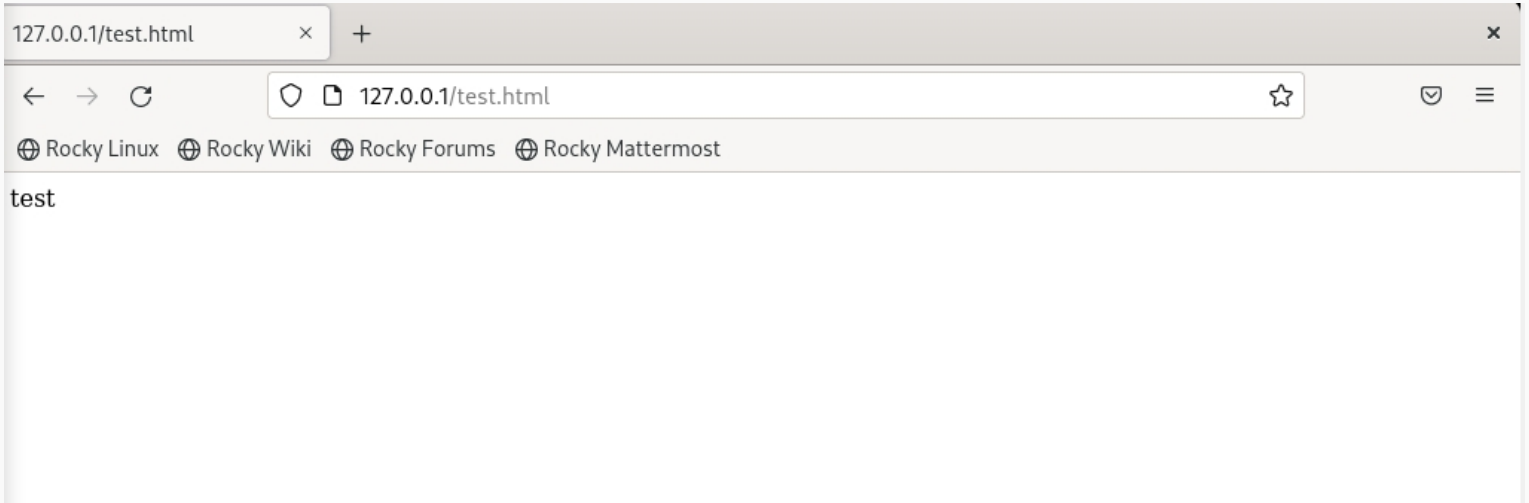

Figure 12: Открытие файла через браузер

Результат выполнения лабораторной работы

Изменение контекста файла test.html с httpd_sys_content_t на samba_share_t, проверка правильность изменения контекста:

```
[root@10 ~]# chcon -t samba_share_t /var/www/html/test.html
[root@10 ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 13: Изменение контекста файла

Результат выполнения лабораторной работы

Попытка получения доступа к измененному файлу через веб-сервер:

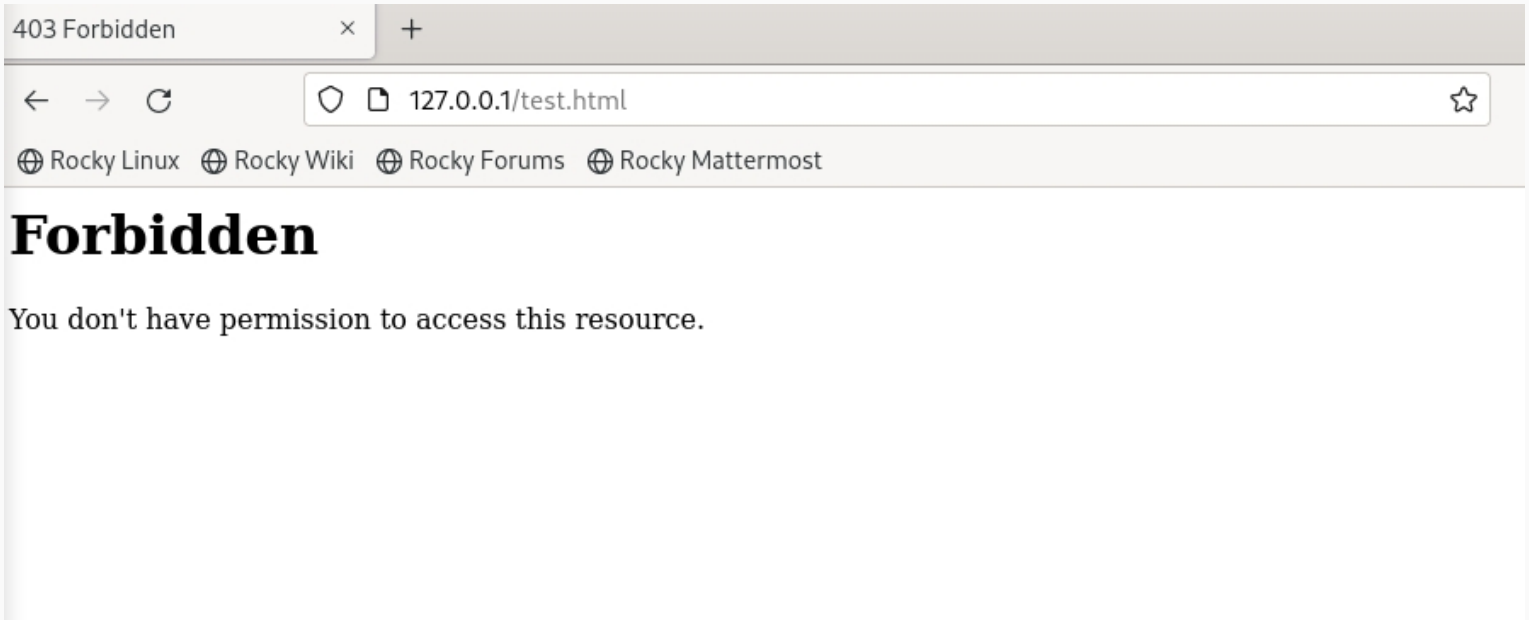

Figure 14: Сообщение об ошибке доступа

Результат выполнения лабораторной работы

Просмотр log-файлов веб-сервера Apache и системного log-файла:

```
[root@10 ~]# tail /var/log/messages
Oct 11 15:23:42 localhost setroubleshoot[42474]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess 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 lab
el should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been sto
pped due to insufficient permissions to access a parent directory in which case try to change the foll
owing command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Plugin
 public_content (7.83 confidence) suggests   *******************#012#012If you want to treat test.htm
l as public content#012Then you need to change the label on test.html to public_content_t or public_co
ntent_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restore
con -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 fi
le by default.#012Then you should report this as a bug.#012You can generate a local policy module to a
llow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | au
dit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 11 15:23:42 localhost setroubleshoot[42474]: failed to retrieve rpm info for /var/www/html/test.ht
ml
Oct 11 15:23:42 localhost setroubleshoot[42474]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 54560a6e-b61f-
43e3-8a7b-7a75abd6d657
Oct 11 15:23:42 localhost setroubleshoot[42474]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess 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 lab
el should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been sto
pped due to insufficient permissions to access a parent directory in which case try to change the foll
owing command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Plugin
 public_content (7.83 confidence) suggests   *******************#012#012If you want to treat test.htm
```

```
[root@10 ~]# tail /var/log/audit/audit.log
type=SERVICE_STOP msg=audit(1665494203.759:280): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syste
m_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=
? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1665497818.100:281): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal
=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1665497818.101:282): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syste
m_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=
? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1665501005.008:283): prog-id=69 op=LOAD
type=SERVICE_START msg=audit(1665501005.162:284): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syst
em_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res
=success'UID="root" AUID="unset"
type=USER_AUTH msg=audit(1665501009.258:285): pid=43817 uid=0 auid=1000 ses=2 subj=system_u:system_r:xdm_t:s0-s
0:c0.c1023 msg='op=PAM:authentication grantors=pam_usertype,pam_localuser,pam_unix,pam_gnome_keyring acct="kpbu
rdina" exe="/usr/libexec/gdm-session-worker" hostname=10.0.2.15 addr=? terminal=/dev/tty1 res=success'UID="root
" AUID="kpburdina"
type=USER_ACCT msg=audit(1665501009.334:286): pid=43817 uid=0 auid=1000 ses=2 subj=system_u:system_r:xdm_t:s0-s
0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="kpburdina" exe="/usr/libexec/gdm-sessio
n-worker" hostname=10.0.2.15 addr=? terminal=/dev/tty1 res=success'UID="root" AUID="kpburdina"
type=CRED_REFR msg=audit(1665501009.338:287): pid=43817 uid=0 auid=1000 ses=2 subj=system_u:system_r:xdm_t:s0-s
0:c0.c1023 msg='op=PAM:setcred grantors=pam_localuser,pam_unix,pam_gnome_keyring acct="kpburdina" exe="/usr/lib
exec/gdm-session-worker" hostname=10.0.2.15 addr=? terminal=/dev/tty1 res=success'UID="root" AUID="kpburdina"
type=SERVICE_STOP msg=audit(1665501035.788:288): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:syste
m_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=
```

Результат выполнения лабораторной работы

Запуск веб-сервера Apache на прослушивание TCP-порта:

```
[root@10 ~]# gedit /etc/httpd/httpd.conf
```

Figure 15: Открытие файла на редактирование

При перезапуске сервера после смены строки с прослушиванием, он не будет работать, поскольку сервер настроен на обределенную частоту прослушки и не сможет быть подключен с другими параметрами.

Результат выполнения лабораторной работы

Анализ log-файлов:

```
[root@10 ~]# tail -n1 /var/log/messages
Oct 11 18:25:17 localhost journal[44192]: Set document metadata failed: Unable to set metadata key
[root@10 ~]# tail -n1 /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[root@10 ~]# tail -n1 /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or directory
[root@10 ~]# tail -n1 /var/log/audit/audit.log
type=BPF msg=audit(1665501878.648:295): prog-id=70 op=UNLOAD
```

Figure 16: Анализ log-файлов

Результат выполнения лабораторной работы

Проверка списка команд, вводимых портом:

```
[root@10 ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@10 ~]# semanage port -a -t http_port_t -p tcp 80
ValueError: Port tcp/80 already defined
[root@10 ~]# 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
```

Figure 17: Команда semanage port

Результат выполнения лабораторной работы

Возвращение контекста httpd_sys_content__t к файлу test.html:

```
[root@10 ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Figure 18: Возвращение контекста

Удаление привязки http_port_t к 81 порту и удаление файла test.html:

```
[root@10 ~]# semanage port -d -t http_port_t -p tcp 81
```

Figure 19: Удаление привязки к порту 81

```
[root@10 ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@10 ~]# cd /var/www/html
[root@10 html]# ls
```

Figure 20: Удаление файла test.html

Выводы

Выводы

1. Развили навыки администрирования ОС Linux;
2. Получили практическое знакомство с технологией SELinux;
3. Проверили работу SELinux на практике совместно с веб-сервером Apache.