

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Ле Тиен Винь

Содержание

I. Цель работы	1
II. Выполнение работы	1
1. Подготовка лабораторного стенда	1
2. Выполнение работы.....	2
III. Вывод	7

I. Цель работы

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

II. Выполнение работы

1. Подготовка лабораторного стенда

- Задать параметр ServerName в конфигурационном файле /etc/httpd/httpd.conf.

```
ServerAdmin root@localhost
```

```
#  
# ServerName gives the name and port that the server uses to identify itself.  
# This can often be determined automatically, but we recommend you specify  
# it explicitly to prevent problems during startup.  
#  
# If your host doesn't have a registered DNS name, enter its IP address here.  
#  
ServerName test.ru
```

- Проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

```
[root@lvtinh ltvinh]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@lvtinh ltvinh]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@lvtinh ltvinh]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
[root@lvtinh ltvinh]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
```

2. Выполнение работы

- Убедиться, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[root@ltvinh ~]$ getenforce
Enforcing
[root@ltvinh ~]$ 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
```

- Проверять, что услуга `httpd` работает. Если она не работает, то запустить её с параметром `start`.

```
[root@ltvinh ~]$ systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ltvinh ~]$ systemctl start httpd
```

```
[root@ltvinh ~]$ 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 Mon 2024-10-07 00:31:04 MSK; 26s ago
     Docs: man:httpd.service(8)
   Main PID: 41880 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
   Tasks: 177 (limit: 23036)
  Memory: 28.1M
    CPU: 71ms
   CGroup: /system.slice/httpd.service
           └─41880 /usr/sbin/httpd -DFOREGROUND
             └─41881 /usr/sbin/httpd -DFOREGROUND
               └─41882 /usr/sbin/httpd -DFOREGROUND
                 └─41883 /usr/sbin/httpd -DFOREGROUND
                   └─41884 /usr/sbin/httpd -DFOREGROUND

Oct 07 00:31:04 ltvinh.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 07 00:31:04 ltvinh.localdomain httpd[41880]: Server configured, listening on
Oct 07 00:31:04 ltvinh.localdomain systemd[1]: Started The Apache HTTP Server.
```

- Использовать команду `ps auxZ | grep httpd`, найти веб-сервер Apache в списке процессов. В нем находится контекст безопасности `"system_u:system_r:httpd_t:s0"`, где:
 1. `system_u` — это системный пользователь, который обычно используется для системных служб, управляемых SELinux.

2. `system_r` — это системная роль, которая позволяет процессам выполнять различные задачи на системном уровне.
3. `httpd_t` — это тип, используемый Apache HTTP Server (`httpd`).
4. `s0` — это уровень безопасности по умолчанию в SELinux, обычно связанный с несекретными данными.

```
[root@ltvinh ltvinh]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      41880  0.0  0.3  20152 11404 ?        Ss   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41881  0.0  0.1  22032  7100 ?        S    00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41882  0.0  0.4 1571340 17256 ?        Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41883  0.0  0.3 1440204 13144 ?        Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41884  0.0  0.2 1440204 10900 ?        Sl   00:31   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 root  42103  0.0  0.0 221664 2176 pts/0 S+   00:32   0:00 grep --color=auto httpd
```

- Посмотреть текущее состояние переключателей SELinux для Apache с помощью команды.

```
[root@ltvinh ltvinh]# 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
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_unified	off
httpd_use_cifs	off
httpd_use_fusefs	off
httpd_use_gpg	off
httpd_use_nfs	off
httpd_use_opencryptoki	off

- Посмотреть статистику по политике с помощью команды `seinfo`, результат даёт количество пользователей, типов, ролей и т.д.

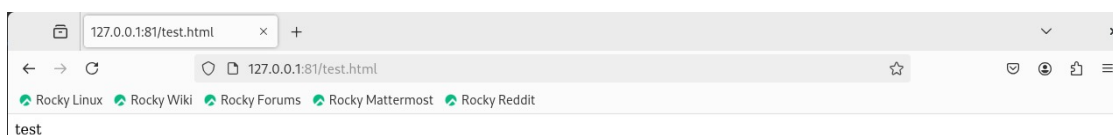
```
[root@ltvinh ltvinh]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  135      Permissions:              457
Sensitivities:            1        Categories:              1024
Types:                    5145     Attributes:               259
Users:                    8         Roles:                   15
Booleans:                 356     Cond. Expr.:             388
Allow:                    65504    Neverallow:               0
Auditallow:               176     Dontaudit:               8682
Type_trans:               271770   Type_change:              94
Type_member:               37      Range_trans:             5931
Role allow:                40      Role_trans:              417
Constraints:              70      Validatetrans:            0
MLS Constrains:           72      MLS Val. Tran:            0
Permissives:               4       Polcap:                   6
Defaults:                 7       Typebounds:               0
Allowxperm:                0      Neverallowxperm:          0
Auditallowxperm:           0      Dontauditxperm:           0
Ibendportcon:              0      Ibkeycon:                 0
Initial SIDs:              27      Fs_use:                   35
Genfscon:                  109     Portcon:                  665
Netifcon:                  0       Nodecon:                  0
```

- Создать от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания.

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

- Обратиться к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.



- Проверить контекст файла `test.html` можно командой `ls -Z /var/www/html/test.html`.
1. Поскольку по умолчанию пользователи не ограничены, созданный нами файл `test.html` был сопоставлен с SELinux, пользователем `unconfined_u`

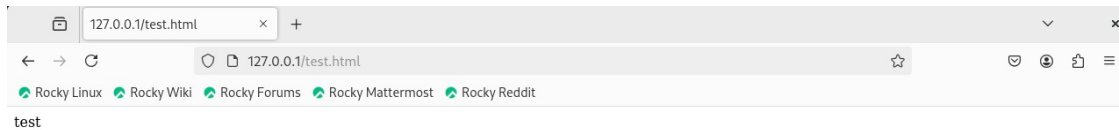
2. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и в сетевых файловых системах
3. Тип `httpd_sys_content_t` позволяет процессу `httpd` получать доступ к файлу типа, с ним мы получили доступ к файлу при доступе к нему через браузер

```
[root@ltvinh ltvinh]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct  7 00:45 /var/www/html/test.html
```

- Изменить контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`, которого процесс `httpd` не имеет доступа.

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

- Попробовать ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.



- Попробовать запустить веб-сервер Apache на прослушивание TCP-порта 81 и убедиться, что порт 81 появился в списке.

```
Listen 81
```

```
[root@ltvinh ltvinh]# 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
```

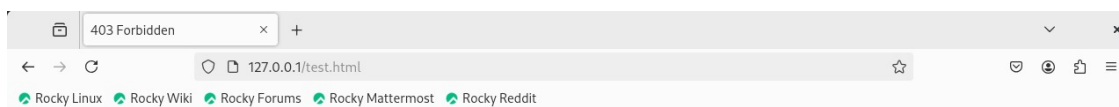
- Выполнять перезапуск веб-сервера Apache и проанализировать лог-файлы.

```
Oct 7 00:53:35 ltvinh systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 7 00:53:35 ltvinh systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 7 00:57:16 ltvinh systemd[1]: Stopping The Apache HTTP Server...
Oct 7 00:57:17 ltvinh systemd[1]: httpd.service: Deactivated successfully.
Oct 7 00:57:17 ltvinh systemd[1]: Stopped The Apache HTTP Server.
Oct 7 00:57:17 ltvinh systemd[1]: Starting The Apache HTTP Server...
Oct 7 00:57:17 ltvinh httpd[43317]: Server configured, listening on: port 81
Oct 7 00:57:17 ltvinh systemd[1]: Started The Apache HTTP Server.
```

- Вернуть контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`.

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

- Попробовать получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.



Forbidden

You don't have permission to access this resource.

- Удалить файл `/var/www/html/test.html`.

III. ВЫВОД

После работы я получил практическое знакомство с технологией SELinux и развил навыки работы с ним.