Лабораторная работа №6

Мандатное разграничение прав в Linux

Тазаева Анастасия Анатольевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Создание программы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. 1). Запустила веб-сервис Apache (рис. 2).

```
[aatazaeva@aatazaeva ~]$ getenforce
Permissive
[aatazaeva@aatazaeva ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

```
○ httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.serv
     Active: inactive (dead)
       Docs: man:httpd.service(8)
~
~
~
~
~
~
lines 1-4/4 (END)
[aatazaeva@aatazaeva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
```

2. Определила его контест безопасности (рис. 3). Посмотрела текущее состояние переключателей SELinux (рис. 4).

```
[aatazaeva@aatazaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       8178  0.0  0.1  21104 11248 ?        Ss   14:17
   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     8185  0.0  0.0  22980  7252 ?        S    14:17
   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     8190  0.0  0.1 982400 11120 ?        Sl   14:17
   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     8191  0.0  0.1 982400 11120 ?        Sl   14:17
   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     8192  0.0  0.1 1113536 13308 ?       Sl   14:17
   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aatazae+ 8402 0.0  0.0 221688 2304 pt
s/1 S+ 14:19   0:00 grep --color=auto httpd
```

```
[root@aatazaeva html]# sestatus -b | gr
httpd_anon_write
httpd_builtin_scripting
httpd_can_check_spam
httpd_can_connect_ftp
httpd_can_connect_ldap
httpd_can_connect_mythtv
httpd_can_connect_zabbix
httpd_can_manage_courier_spool
httpd_can_network_connect
httpd_can_network_connect_cobbler
httpd_can_network_connect_db
httpd_can_network_memcache
httpd_can_network_relay
httpd_can_sendmail
httpd_dbus_avahi
httpd_dbus_sssd
```

3. Посмотрела статистику по политике с помощью команды seinfo (рис. 5).

```
[aatazaeva@aatazaeva ~]$ 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:              5190    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            358    Cond. Expr.:         390
  Allow:             66298    Neverallow:            0
  Auditallow:          178    Dontaudit:          8723
  Type_trans:       274477    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           6    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
```

Рис. 2.1: Статистика по политике

4. Определила тип файлов и поддиректорий, находящихся в директории /var/www, обратилась к файлу через веб-сервер (рис. 6 и рис. 7)

```
[aatazaeva@aatazaeva ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 авг 12 16:20 html
```

Рис. 2.2: Типы файлов и поддиректории

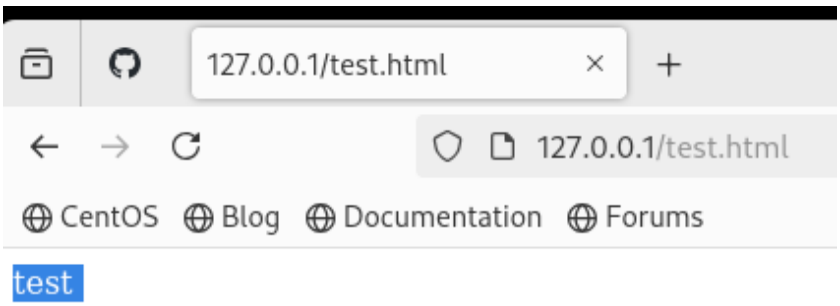

Рис. 2.3: Запуск в браузере

5. Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой (рис. 8), к которому процесс httpd не должен иметь доступа, попробовала ещё раз получить доступ к файлу через веб-сервер, интересно, что у меня доступ был разрешен и я всё также видела запись “тест”. Предположить не могла как исправить это и потому часть пунктов опускаю в лабораторной работе.

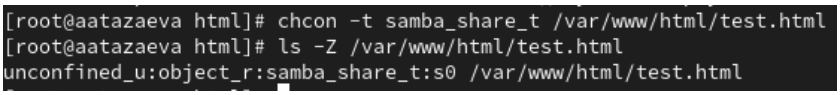

Рис. 2.4: Изменение контекста файла

6. Просмотрела log-файлы веб-сервера Apache (рис. 9).

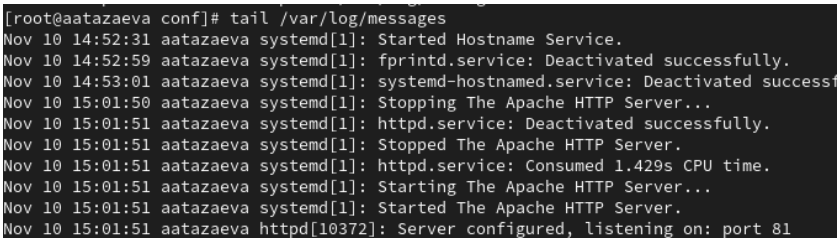

Рис. 2.5: Лог файлы

7. Не удалось открыть файл через 81 порт, так что контекст был возвращен и привязка к порту 81 была удалена, также был удален файл html (рис. 10)

```
[root@aatazaeva ~]# semanage  port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@aatazaeva ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? yes
```

Рис. 2.6: Удаление привязки к порту, удаление файла

3 Выводы

Я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux, а также проверила работу SELinux на практике совместно с веб-сервером Apache.