Отчёт по лабораторной работе 6

Невзоров Дмитрий Сергеевич

2021

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

- Лабораторная работа подразумневает последовательное выполнение команд, используя разные расширенные атрибуты

Выполнение лабораторной работы

- Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*

```
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
```

Рис.1

Обратимся к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает: *service httpd status*

```
[root@Nevzorov Nevzorov1]# service httpd status
httpd (pid  8834) выполняется...
[root@Nevzorov Nevzorov1]#
```

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности, используем команду *ps auxZ | grep httpd*

```
[root@Nevzorov Nevzorov1]# ps auxZ | grep httpd
unconfined_u:system_r:httpd_t:s0 root     8834  0.0  0.3  11668  3508 ?        S
s   06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8837  0.0  0.2  11804  2896 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8838  0.0  0.2  11804  2960 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8839  0.0  0.2  11804  2888 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8840  0.0  0.2  11804  2888 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8841  0.0  0.2  11668  2208 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8842  0.0  0.2  11668  2224 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8843  0.0  0.2  11668  2208 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   8844  0.0  0.2  11668  2208 ?        S
    06:49   0:00 /usr/sbin/httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 9208 0.0  0.0 4444 82
0 pts/3 S+ 07:43   0:00 grep httpd
[root@Nevzorov Nevzorov1]#
```

Выполнение лабораторной работы

- Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды *sestatus –b | grep httpd*

```
[root@Nevzorov Nevzorov1]# sestatus -b | grep httpd
allow_httpd_anon_write                      off
allow_httpd_mod_auth_ntlm_winbind           off
allow_httpd_mod_auth_pam                    off
allow_httpd_sys_script_anon_write           off
httpd_builtin_scripting                     on
httpd_can_check_spam                        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                            on
httpd_dbus_sssd                             off
httpd_enable_cgi                            on
httpd_enable_ftp_server                     off
httpd_enable_homedirs                       off
httpd_execmem                               off
httpd_manage_ipa                            off
httpd_read_user_content                     off
httpd_run_preupgrade                        off
httpd_run_stickshift                        off
httpd_serve_cobbler_files                   off
httpd_setrlimit                             off
httpd_ssi_exec                              off
httpd_tmp_exec                              off
httpd_tty_comm                              on
httpd_unified                               on
httpd_use_cifs                              off
httpd_use_fusefs                            off
httpd_use_gpg                               off
httpd_use_nfs                               off
httpd_use_openstack                         off
httpd_verify_dns                            off
```

Многие из переключателей находятся в положении «off».

Выполнение лабораторной работы

- Посмотрим статистику по политике с помощью команды *seinfo*, также определим множество пользователей, ролей и типов.

```
[root@Nevzorov Nevzorov1 ]# seinfo

Statistics for policy file: /etc/selinux/targeted/policy/policy.24
Policy Version & Type: v.24 (binary, mls)

   Classes:            81    Permissions:       238
   Sensitivities:       1    Categories:       1024
   Types:            3920    Attributes:        295
   Users:               9    Roles:              12
   Booleans:          237    Cond. Expr.:       277
   Allow:          323336    Neverallow:          0
   Auditallow:        141    Dontaudit:      274738
   Type_trans:      42431    Type_change:        38
   Type_member:        48    Role allow:         19
   Role_trans:        386    Range_trans:      6258
   Constraints:        90    Validatetrans:       0
   Initial SIDs:       27    Fs_use:             23
   Genfscon:           84    Portcon:           474
   Netifcon:            0    Nodecon:             0
   Permissives:        90    Polcap:              2
```

Пользователей: 9, ролей: 12, типов: 3920.

1. Определим тип файлов и поддиректорий, находящихся в директории */var/www* с помощью команды *ls -lZ /var/www*

Выполнение лабораторной работы

- создадим от имени суперпользователя html-файл */var/www/html/test.html* следующего содержания:
- **<html>**
- **<body>**test**</body>**
- **</html>**

Выполнение лабораторной работы

1. Изучим справку *man httpd_selinux* и выясним, какие контексты файлов определены для *httpd* и сопоставим их с типом *файла test.html*. Проверим контекст файла командой *ls –Z /var/www/html/test.htm*

```
[root@Nevzorov Nevzorov1 ]# 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@Nevzorov Nevzorov1 ]#
```

1. Изменим контекст файла */var/www/html/test.html* с httpd_sys_content_t на другой, к которому процесс httpd не должен иметь доступа, в нашем случае, на samba_share_t:

1. Попробуем еще раз получить доступ к файлу через веб-сервер, введя в браузере firefox адрес *http://127.0.0.1/test.html*

1. Проанализируем ситуацию, просмотрев log-файлы веб-сервера Apache, системный log-файл и audit.log при условии уже запущенных процессов setroubleshootd и audtd.

```
oot" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1603680602.094:2295): user pid=15699 uid=0 auid=0 ses=28
9 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="root" e
xe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1603680602.094:2296): user pid=15699 uid=0 auid=0 ses=289
 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct="ro
ot" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_ACCT msg=audit(1603681201.119:2297): user pid=15794 uid=0 auid=42949672
95 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accou
nting acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=succe
ss'
type=CRED_ACQ msg=audit(1603681201.120:2298): user pid=15794 uid=0 auid=429496729
5 ses=4294967295 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcre
d acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1603681201.121:2299): pid=15794 uid=0 subj=system_u:system_r
:crond_t:s0-s0:c0.c1023 old auid=4294967295 new auid=0 old ses=4294967295 new ses
=290
type=USER_START msg=audit(1603681201.121:2300): user pid=15794 uid=0 auid=0 ses=2
90 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open acct="r
oot" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1603681201.197:2301): user pid=15794 uid=0 auid=0 ses=29
0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="root" e
xe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1603681201.197:2302): user pid=15794 uid=0 auid=0 ses=290
 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close acct="ro
ot" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
```

- Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в */etc/services*), заменив в файле */etc/httpd/conf/httpd.conf* строчку *Listen 80* на *Listen 81.*

Выполнение лабораторной работы

```
[root@Nevzorov Nevzorov1]# semanage port -d -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 определен на уровне политики и не может быть удал
ен
[root@Nevzorov Nevzorov1]#
```

1. Удалим привязку http_port_t к 81 порту: *semanage port –d –t http_port_t –p tcp 81*. Данную команду выполнить невозможно на моей версии CentOS, поэтому получаем ошибку.

- Удалим файл */var/www/html/test.html*: *rm /var/www/html/test.html*

```
[root@Nevzorov Nevzorov1]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@Nevzorov Nevzorov1]#
```

Вывод

- Я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.

Спасибо за внимание!