Лабораторная работа № 6

Казакова Виктория Алексеевна

2023, Москва

Цели

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Задачи

1. Настроить и запустить сервер Apache.
2. Изучить технологию Selinux1.

Ход работы

Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted

```
[root@victoria22 victoria22]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@victoria22 victoria22]# setenforce 1
[root@victoria22 victoria22]# getenforce
Enforcing
[root@victoria22 victoria22]# 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
Max kernel policy version:      31
[root@victoria22 victoria22]#
```

Рис. 1: Конфигурация SELinux

Ход работы

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что он работает

```
[victoria22@victoria22 ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[victoria22@victoria22 ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[victoria22@victoria22 ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Сб 2023-10-14 14:56:26 MSK; 3s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 14316 (httpd)
   Status: "Processing requests..."
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─14316 /usr/sbin/httpd -DFOREGROUND
           ├─14328 /usr/sbin/httpd -DFOREGROUND
           ├─14329 /usr/sbin/httpd -DFOREGROUND
           ├─14330 /usr/sbin/httpd -DFOREGROUND
           ├─14331 /usr/sbin/httpd -DFOREGROUND
           └─14332 /usr/sbin/httpd -DFOREGROUND

окт 14 14:56:26 victoria22.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 14:56:26 victoria22.localdomain httpd[14316]: AH00558: httpd: Could not re...e
окт 14 14:56:26 victoria22.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Ход работы

Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности

```
system_u:system_r:httpd_t:s0    apache   14328  0.0  0.0 232528  3160 ?        S    14:56   0:00
 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   14329  0.0  0.0 232528  3160 ?        S    14:56   0:00
 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   14330  0.0  0.0 232528  3160 ?        S    14:56   0:00
 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   14331  0.0  0.0 232528  3160 ?        S    14:56   0:00
 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache   14332  0.0  0.0 232528  3160 ?        S    14:56   0:00
 /usr/sbin/httpd -DFOREGROUND
```

Рис. 3: Контекст безопасности веб-сервера Apache

Ход работы

Посмотрела текущее состояние переключателей SELinux для Apache

```
[victoria22@victoria22 ~]$ 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_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                     on
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
```

Ход работы

Посмотрела статистику по политике с помощью команды seinfo

```
[victoria22@victoria22 ~]$ seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

   Classes:            130    Permissions:       272
   Sensitivities:        1    Categories:       1024
   Types:             4793    Attributes:        253
   Users:                8    Roles:              14
   Booleans:           316    Cond. Expr.:       362
   Allow:           107834    Neverallow:          0
   Auditallow:         158    Dontaudit:       10022
   Type_trans:       18153    Type_change:        74
   Type_member:         35    Role allow:         37
   Role_trans:         414    Range_trans:      5899
   Constraints:        143    Validatetrans:       0
   Initial SIDs:        27    Fs_use:             32
   Genfscon:           103    Portcon:           614
   Netifcon:             0    Nodecon:             0
   Permissives:          0    Polcap:              5

[victoria22@victoria22 ~]$
```

Ход работы

Определила тип файлов, находящихся в директории /var/www/html

Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html

Ход работы

Создала от имени суперпользователя html-файл /var/www/html/test.html

```
[root@victoria22 victoria22]# touch /var/www/html/test.html
[root@victoria22 victoria22]# mc
```

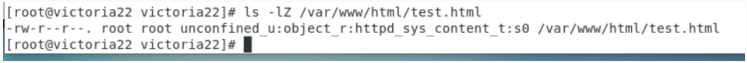
Рис. 6: Создание файла /var/www/html/test.html

Ход работы

Рис. 7: Создание файла /var/www/html/test.html

Ход работы

Проверила контекст созданного файла



По умолчанию присваивается контекст unconfined_u:object_r:httpd_sys_content_t:s0

Ход работы

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён

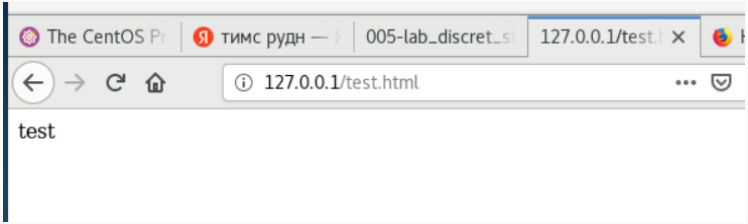


Рис. 8: Файл test.html в браузере

Ход работы

Изучила справку man httpd_selinux и выяснила, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t

```
[root@victoria22 victoria22]# chcon -t samba_share_t /var/www/html/test.html
[root@victoria22 victoria22]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@victoria22 victoria22]#
```

Рис. 9: Изменение контекста

Ход работы

Попробовала ещё раз получить доступ к файлу через веб-сервер. В ответ получила запись Forbidden. You don’t have permission to access /test.html on this server Просмотрела log-файлы веб-сервера Apache и системный лог-файл

```
[root@victoria22 victoria22]# ls -l /var/www/html/test.htm
ls: невозможно получить доступ к /var/www/html/test.htm: Нет такого файла или каталога
[root@victoria22 victoria22]# tail /var/log/messages
Oct 14 15:10:02 victoria22 systemd: Started Session 35 of user root.
Oct 14 15:10:02 victoria22 systemd: Removed slice User Slice of root.
Oct 14 15:11:30 victoria22 org.gnome.Shell.desktop: Window manager warning: Buggy client sent a _NET_ACTIV
E_WINDOW message with a timestamp of 0 for 0x3c000f8 (test.html )
Oct 14 15:16:56 victoria22 dbus[757]: [system] Activating via systemd: service name='net.reactivated.Fprin
t' unit='fprintd.service'
Oct 14 15:16:56 victoria22 systemd: Starting Fingerprint Authentication Daemon...
Oct 14 15:16:56 victoria22 dbus[757]: [system] Successfully activated service 'net.reactivated.Fprint'
Oct 14 15:16:56 victoria22 systemd: Started Fingerprint Authentication Daemon.
Oct 14 15:17:01 victoria22 su: (to root) victoria22 on pts/1
Oct 14 15:17:01 victoria22 dbus[757]: [system] Activating service name='org.freedesktop.problems' (using s
ervicehelper)
Oct 14 15:17:01 victoria22 dbus[757]: [system] Successfully activated service 'org.freedesktop.problems'
[root@victoria22 victoria22]#
```

Мне не удалось получить доступ к файлу из-за измененного контекста.

Ход работы

Выполнила перезапуск веб-сервера. Сбоя не произошло Проанализировала лог-файлы

Ход работы

Выполнила команду semanage port -a -t http_port_t -p tcp 81. После этого проверила список портов командой semanage port -l | grep http_port_t

```
[root@victoria22 victoria22]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]

                {import,export,login,user,port,ibpkey,ibendport,interface,module
,node,fcontext,boolean,permissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@victoria22 victoria22]# 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
[root@victoria22 victoria22]#
```

Рис. 10: Попытка добавления порта 81 в список и вывод списка допустимых портов

Ход работы

Попробовала удалить привязку http_port_t к 81. Удаление невозможно. Удалила файл /var/www/html/test.html

```
[root@victoria22 victoria22]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@victoria22 victoria22]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@victoria22 victoria22]#
```

Рис. 11: Попытка удаления привязки к порту 81. Удаление файла /var/www/html/test.html

Результаты

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux1. Проверена работа SELinx на практике совместно с веб-сервером Apache.