Лабораторная работа №6: Дискреционное разграничение прав в Linux. Расширенные атрибуты

дисциплина: Информационная безопасность

Швец Сергей Сергеевич

2021, 27 november

Цель работы

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

Выполнение работы

Установка httpd

```
[root@Shvets html]# yum install httpd -y
Последняя проверка окончания срока действия метаданных: 2:27:34 назад, Сб 27 ноя 2021 1
8:52:19.
Зависимости разрешены.
================================================================================
 Пакет            Архитектура
                         Версия                                  Репозиторий
                                                                          Размер
================================================================================
Установка:
 httpd            x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream 1.4 M
```

Figure 1: httpd

Вход в систему

Войдите в систему с полученными учётными данными и убедитесь, что

SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

```
[shvets@Shvets ~]$ getenforce
Enforcing
[shvets@Shvets ~]$ setstatus
bash: setstatus: команда не найдена...
[shvets@Shvets ~]$ 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: вход

Обращение

Обращение с помощью браузера к веб-серверу, запущенному на компьютере

```
[shvets@Shvets ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
[shvets@Shvets ~]$ -start service httpd status
```

Figure 3: обращение к веб-серверу

Контекст

Определение контекста безопасности.

```
[shvets@Shvets ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 shvets 5256 0.0  0.0 12136 1044 p
ts/0 R+ 20:05   0:00 grep --color=auto httpd
```

Figure 4: Контекст безопасности

Состояние

Текущее состояние переключателей SELinux для Apache.

```
Without options, show SELinux status.
[shvets@Shvets ~]$ 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                      off
httpd_manage_ipa                             off
httpd_mod_auth_ntlm_winbind                  off
```

Figure 5: просмотр состояния

Файлы и поддиректории

Определение типа файлов и поддиректорий, находящихся в директории.

```
[root@Shvets html]# ls -LZ /var/www/html
[root@Shvets html]# /var/www/html
bash: /var/www/html: Это каталог
```

Figure 6: Расширенные атрибуты

Создание файла test.html

Создание файла test.html

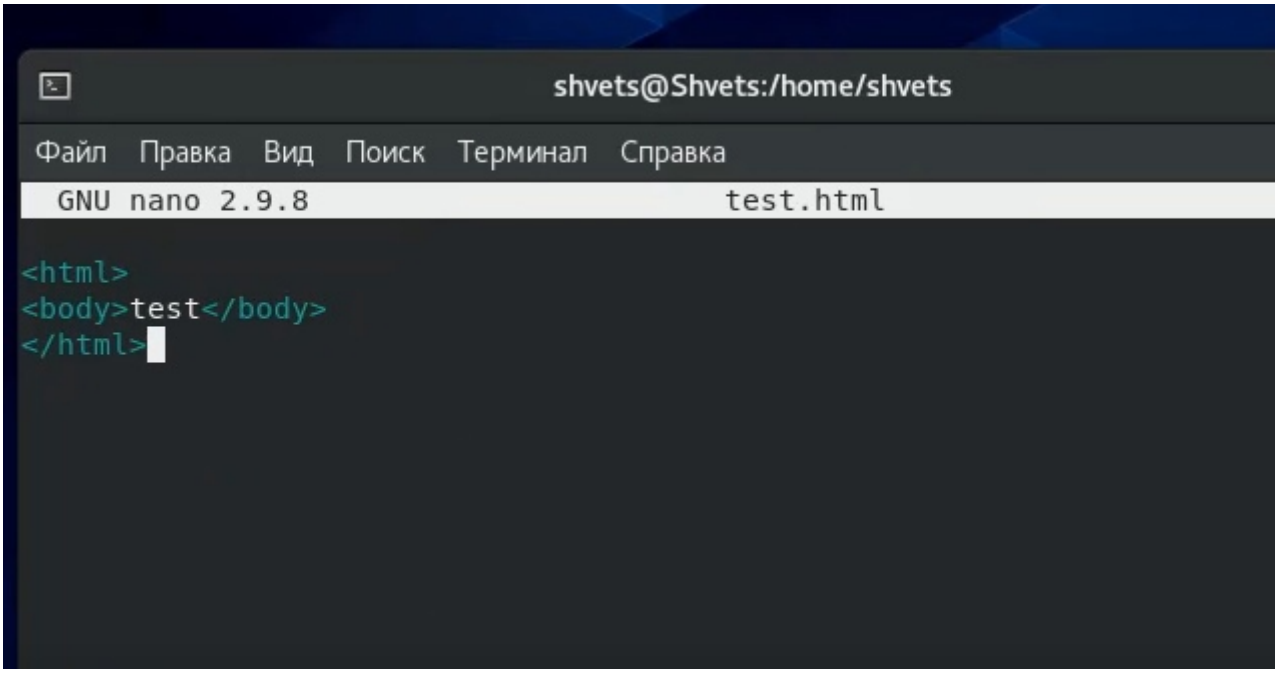

Figure 7: test.html

Log-файл

Просмотр системного log-файла.

```
[root@Shvets html]# tail /var/log/messages
Nov 27 21:20:14 Shvets systemd[1]: Started /usr/bin/systemctl start man-db-cache-update
.
Nov 27 21:20:15 Shvets systemd[1]: Starting man-db-cache-update.service...
Nov 27 21:20:15 Shvets systemd[1]: Reloading.
Nov 27 21:20:22 Shvets systemd[1]: man-db-cache-update.service: Succeeded.
Nov 27 21:20:22 Shvets systemd[1]: Started man-db-cache-update.service.
Nov 27 21:20:22 Shvets systemd[1]: run-ra8c1dade472541db814731337e0fadd8.service: Succe
eded.
Nov 27 21:22:30 Shvets cupsd[968]: REQUEST localhost - - "POST / HTTP/1.1" 200 185 Rene
w-Subscription successful-ok
Nov 27 21:24:35 Shvets org.gnome.Shell.desktop[1648]: libinput error: event4  - Virtual
Box mouse integration: client bug: event processing lagging behind by 11ms, your system
 is too slow
Nov 27 21:24:35 Shvets org.gnome.Shell.desktop[1648]: libinput error: event4  - Virtual
Box mouse integration: client bug: event processing lagging behind by 13ms, your system
 is too slow
Nov 27 21:24:35 Shvets org.gnome.Shell.desktop[1648]: libinput error: event4  - Virtual
Box mouse integration: WARNING: log rate limit exceeded (5 msgs per 60min). Discarding
future messages.
```

Figure 8: log-файл

Попытка перезапуска

Попытка перезапуска сервера

```
Redirecting to /bin/systemctl stop httpd.service
[root@Shvets html]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@Shvets html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Log-файлы

tail -nl /var/log/messages.

```
[root@Shvets html]# tail -n1 /var/log/messages
Nov 27 21:35:59 Shvets httpd[42596]: Server configured, listening on: port 80
```

Список портов

semanage port -l | grep http_port_t.

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

Выводы

Я ознакомился с базовыми с технологией SELinux. Развил навыки администратора и проверил работу SELinux на практике.