

Лабораторная работа №6

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна

Содержание

1	Техническое оснащение:	5
2	Цели и задачи работы	6
2.1	Цель	6
2.2	Задачи	6
3	Теоретическое введение и подготовка лабораторного стенда	7
4	Выполнение лабораторной работы [1]	9
5	Выводы по проделанной работе	21
5.1	Вывод	21
6	Список литературы	22

Список иллюстраций

4.1	Проверим SELinux	9
4.2	Проверяем	10
4.3	Контекст безопасности	10
4.4	Текущее состояние переключателей SELinux для Apache	11
4.5	Статистика по политике	11
4.6	Типы поддиректорий и файлов в директории /var/www	12
4.7	Тип файлов в директории /var/www/html	12
4.8	Определим права на файл	12
4.9	Создадим файл	13
4.10	Определим контекст	13
4.11	http://127.0.0.1/test.html	14
4.12	Контексты файлов, определённые для SELinux	15
4.13	Изменяем контекст файла	15
4.14	http://127.0.0.1/test.html	16
4.15	log-файлы	16
4.16	Замена строки	17
4.17	Перезапуск веб-сервера	17
4.18	Список портов	18
4.19	Веб-сервер работает	19
4.20	http://127.0.0.1:81/test.html	19
4.21	Исправляем конфигурационный файл	19
4.22	Удаляем привязку	20
4.23	Удаляем файл	20

Список таблиц

1 Техническое оснащение:

- Персональный компьютер с операционной системой Windows 10;
- Планшет для записи видеосопровождения и голосовых комментариев;
- Microsoft Teams, использующийся для записи скринкаста лабораторной работы;
- Приложение Rucharm для редактирования файлов формата *md*;
- *pandoc* для конвертации файлов отчётов и презентаций.

2 Цели и задачи работы

2.1 Цель

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

2.2 Задачи

1. Подготовить лабораторный стенд;
2. Запустить Apache в системе;
3. Создать небольшой веб-сервер;
4. Посмотреть различные варианты настроек сервера и изучить реакции на изменение этих настроек.

3 Теоретическое введение и подготовка лабораторного стенда

HTTP-сервер Apache — самый широко используемый веб-сервер в мире. Он имеет множество мощных функций, включая динамически загружаемые модули, надежную поддержку различных медиаформатов и интеграцию с другим популярным программным обеспечением.

Apache доступен в используемых по умолчанию репозиториях программного обеспечения CentOS, т. е. вы можете установить его с помощью менеджера пакетов yum.

Порядок настройки машины для использования Apache:

```
sudo yum update httpd
sudo yum install httpd
sudo yum install firewalld
sudo systemctl start firewalld
sudo firewall-cmd --permanent --add-service=ssh
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --reload
sudo systemctl enable firewalld
```

В файле /etc/httpd/httpd.conf необходимо задать:

```
ServerName test.ru
```

Также необходимо проследить, чтобы пакетный фильтр был отключён. Отключить фильтр можно командами:

```
sudo iptables -F
```

```
sudo iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```


4 Выполнение лабораторной работы [1]

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команды sestatus. (4.1)

sestatus

```
[vemanaeva@vemanaeva ~]$ 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
```

Рис. 4.1: Проверим SELinux

2. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает (4.2)

```
sudo systemctl start httpd
```

```
service httpd status
```

```
[vmanaeva@vmanaeva ~]$ sudo systemctl start httpd
[vmanaeva@vmanaeva ~]$ 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 14:38:31 MSK; 2s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3617 (httpd)
    Status: "Processing requests..."
      Tasks: 6
    CGroup: /system.slice/httpd.service
            └─3617 /usr/sbin/httpd -DFOREGROUND
            └─3621 /usr/sbin/httpd -DFOREGROUND
            └─3622 /usr/sbin/httpd -DFOREGROUND
            └─3623 /usr/sbin/httpd -DFOREGROUND
            └─3624 /usr/sbin/httpd -DFOREGROUND
            └─3625 /usr/sbin/httpd -DFOREGROUND

окт 14 14:38:31 vmanaeva.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 14:38:31 vmanaeva.localdomain httpd[3617]: AH00558: httpd: could not reliably determine the server's fully qualified domain name, using vmanaeva.localdomain. Set the 'ServerName' dire... this message
окт 14 14:38:31 vmanaeva.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[vmanaeva@vmanaeva ~]$
```

Рис. 4.2: Проверяем

3. Найдём веб-сервер Apache в списке процессов и определим его контекст безопасности (4.3)

```
ps auxZ | grep httpd
```

```
ps -eZ | grep httpd
```

```
[vmanaeva@vmanaeva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3617 0.3 0.2 230444 5224 ? Ss 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3621 0.0 0.1 232528 3160 ? S 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3622 0.0 0.1 232528 3160 ? S 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3623 0.0 0.1 232528 3160 ? S 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3624 0.0 0.1 232528 3160 ? S 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3625 0.0 0.1 232528 3160 ? S 14:38 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vmanae+ 3661 0.0 0.0 112832 972 pts/0 R+ 14:38 0:00 grep --color=auto httpd
[vmanaeva@vmanaeva ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3617 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3621 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3622 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3623 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3624 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3625 ? 00:00:00 httpd
```

Рис. 4.3: Контекст безопасности

4. Посмотрим текущее состояние переключателей SELinux для Apache (4.4)

```
sestatus -bigrep httpd
```

```
[vemanaeva@vemanaeva ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write off
abrt_handle_event off
abrt_upload_watch_anon_write on
antivirus_can_scan_system off
antivirus_use_jit off
auditadm_exec_content on
authlogin_nsswitch_use_ldap off
authlogin_radius off
authlogin_yubikey off
awstats_purge_apache_log_files off
boinc_execmem on
cdrecord_read_content off
cluster_can_network_connect off
cluster_manage_all_files off
cluster_use_execmem off
cobbler_anon_write off
cobbler_can_network_connect off
cobbler_use_cifs off
cobbler_use_nfs off
collectd_tcp_network_connect off
condor_tcp_network_connect off
conman_can_network off
conman_use_nfs off
container_connect_any off
cron_can_relabel off
cron_system_cronjob_use_shares off
cron_userdomain_transition on
cups_execmem off
cvs_read_shadow off
daemons_dump_core off
daemons_enable_cluster_mode off
daemons_use_tcp_wrapper off
daemons_use_tty off
dbadm_exec_content on
```

Рис. 4.4: Текущее состояние переключателей SELinux для Apache

5. Посмотрим статистику по политике, а также определим множество пользо- вателей, ролей и типов (4.5)

seinfo

```
[vemanaeva@vemanaeva ~]$ 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
```

Рис. 4.5: Статистика по политике

6. Определим тип файлов и поддиректорий, находящихся в директории /var/www (4.6)

```
ls -lZ /var/www
```

```
[vemanaeva@vemanaeva ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[vemanaeva@vemanaeva ~]$
```

Рис. 4.6: Типы поддиректорий и файлов в директории /var/www

7. Определим тип файлов, находящихся в директории /var/www/html (4.7)

```
ls -lZ /var/www/html
```

```
[vemanaeva@vemanaeva ~]$ ls -lZ /var/www/html
[vemanaeva@vemanaeva ~]$
```

Рис. 4.7: Тип файлов в директории /var/www/html

8. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html (только суперпользователь) (4.8)

```
ls -l /var/www
```

```
-----
Genfscon: 103 Portcon: 614
Netifcon: 0 Nodecon: 0
Permissives: 0 Polcap: 5
[Superuser can create, others cannot]
[vemanaeva@vemanaeva ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
```

Рис. 4.8: Определим права на файл

9. Создадим от имени суперпользователя html-файл /var/www/html/test.html (4.9)

```
sudo nano /var/www/html/test.html
```

```
<html>
```

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

```
</html>
```



Рис. 4.9: Создадим файл

10. Проверим контекст созданного файла. (4.10)

```
ls -Z /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ 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
```

Рис. 4.10: Определим контекст

11. Обратимся к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”.
Убедимся, что файл был успешно отображён. (4.11)

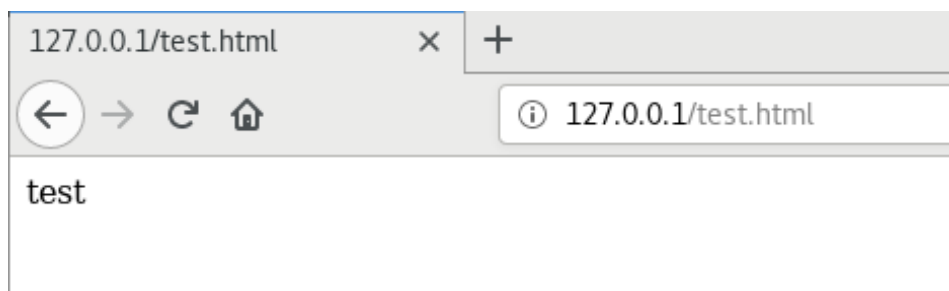


Рис. 4.11: http://127.0.0.1/test.html

12. Изучим справку и выясните, какие контексты файлов определены для httpd.
Сопоставим их с типом файла test.html, проверив контекст файла (4.12)

```
man httpd_selinux  
ls -Z /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ sudo semanage fcontext --li | grep httpd
/usr/*\.*.cgi regular file
/opt/*\.*.cgi regular file
/srv/([^\s]*)/*/*www(/.*)? all files
/srv/([^\s]*)/*/*www/logs(/.*)? all files
/var/www(/.*)? all files
/var/www(/.*)?/logs(/.*)? all files
/etc/glpi(/.*)? all files
/var/www/[^\s]*cgi-bin(/.*)? all files
/etc/horde(/.*)? all files
/etc/htdig(/.*)? all files
/etc/httpd(/.*)? all files
/etc/nginx(/.*)? all files
/etc/drupal.* all files
/etc/z-push(/.*)? all files
/etc/apache(2)?(/.*)? all files
/var/lib/rt(3|4)/data/RT-Shredder(/.*)? all files
/var/lib/dav(/.*)? all files
/var/lib/php(/.*)? all files
/var/lib/svn(/.*)? all files
/var/www/svn(/.*)? all files
/var/run/wsgi.* socket
/var/run/mod.* all files
/etc/ Cherokee(/.*)? all files
/etc/owncloud(/.*)? all files
/etc/lighttpd(/.*)? all files
/srv/gallery2(/.*)? all files
/var/lib/glpi(/.*)? all files
/var/lib/trac(/.*)? all files
/var/log/glpi(/.*)? all files
/var/www/perl(/.*)? all files
/var/cache/rt(3|4)(/.*)? all files
/var/www/html(/.*)?/uploads(/.*)? all files
/var/www/html(/.*)?/wp-content(/.*)? all files
/var/www/html(/.*)?/wp_backups(/.*)? all files
/var/www/html(/.*)?/sites/default/files(/.*)? all files
/var/www/html(/.*)?/sites/default/settings\.*php regular file
/var/run/httpd.* all files
/var/run/nginx.* all files
/var/cache/ssl/*.*.sem regular file
/etc/nextcloud(/.*)? all files
/etc/mock/koji(/.*)? all files
/usr/lib/httpd(/.*)? all files
/var/lib/htdig(/.*)? all files
/var/lib/httpd(/.*)? all files
/var/lib/nginx(/.*)? all files
system_u:object_r:httpd_sys_script_exec_t:s0
system_u:object_r:httpd_sys_script_exec_t:s0
system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:httpd_log_t:s0
system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:httpd_log_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_script_exec_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:httpd_config_t:s0
system_u:object_r:httpd_config_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_config_t:s0
system_u:object_r:httpd_var_lib_t:s0
system_u:object_r:httpd_var_lib_t:s0
system_u:object_r:httpd_var_lib_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_var_run_t:s0
system_u:object_r:httpd_var_run_t:s0
system_u:object_r:httpd_config_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_config_t:s0
system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:httpd_var_lib_t:s0
system_u:object_r:httpd_log_t:s0
system_u:object_r:httpd_sys_script_exec_t:s0
system_u:object_r:httpd_cache_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_run_t:s0
system_u:object_r:httpd_var_run_t:s0
system_u:object_r:httpd_var_run_t:s0
system_u:object_r:httpd_cache_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_sys_rw_content_t:s0
system_u:object_r:httpd_modules_t:s0
system_u:object_r:httpd_sys_content_t:s0
system_u:object_r:httpd_var_lib_t:s0
system_u:object_r:httpd_var_lib_t:s0
```

Рис. 4.12: Контексты файлов, определённые для SELinux

13. Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа (4.13)

```
sudo chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[vemanaeva@vemanaeva ~]$ 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
[vemanaeva@vemanaeva ~]$ █
```

Рис. 4.13: Изменяем контекст файла

14. Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. И получаем сообщение об ошибке `Forbidden`. (4.14)



Forbidden

You don't have permission to access /test.html on this server.

Рис. 4.14: http://127.0.0.1/test.html

15. Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache.
(4.15)

```
ls -l /var/www/html/test.html
```

```
tail /var/log/messages
```

```
venanaev@venanaeva:~$ sudo tail /var/log/messages
bct 14:14:54.03 venanaeva dbus[783]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
bct 14:14:54.04 venanaeva dbus[783]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
bct 14:14:54.04 venanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
bct 14:14:54.04 venanaeva setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 9855aefb-a7c6-4206-bcd5-72205f5aa3bc
bct 14:14:54.04 venanaeva python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012**** Plugin restorecon (92.2 confidence) suggests *****#012#01
2If you want to fix the label.#012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120a#012$ /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (17.83 confidence) suggests *****#012#01
2If you want to fix the label.#012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120a#012$ /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (17.83 confidence) suggests *****#012#01
2If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#0120a#012$ semanage context -a -t public
content_t /var/www/html/test.html.#012#012**** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be
allowed getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120a#012$ allow this access for now by executing:#
$12$ ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012$ semodule -i my-httpd.pp#012
bct 14:14:54.16 venanaeva dbus[783]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
bct 14:14:54.17 venanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
bct 14:14:54.17 venanaeva python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 9855aefb-a7c6-4206-bcd5-72205f5aa3bc
bct 14:14:54.17 venanaeva python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012**** Plugin restorecon (92.2 confidence) suggests *****#012#01
2If you want to fix the label.#012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120a#012$ /sbin/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (17.83 confidence) suggests *****#012#01
2If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#0120a#012$ semanage context -a -t public
content_t /var/www/html/test.html.#012#012**** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be
allowed getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120a#012$ allow this access for now by executing:#
$12$ ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012$ semodule -i my-httpd.pp#012
venanaev@venanaeva:~$
```

Рис. 4.15: log-файлы

16. Запустим веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81
(4.16)

```
nano /etc/httpd/httpd.conf
```



```
GNU nano 2.3.1                               Файл: /etc/httpd/httpd.conf
ServerName test.ru
Listen 81

Имя файла для записи: /etc/httpd/httpd.conf
```

Рис. 4.16: Замена строки

17. Выполним перезапуск веб-сервера Apache (4.17)

```
sudo systemctl start httpd
```

```
[vemanaeva@vemanaeva ~]$ sudo systemctl start httpd
[vemanaeva@vemanaeva ~]$
```

Рис. 4.17: Перезапуск веб-сервера

18. Проанализируем лог-файлы `/var/log/messages`. Также посмотрим файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясним, в каких файлах появились записи (??)

```
tail /var/log/messages
tail /var/log/http/error_log
tail /var/log/http/access_log
tail /var/log/audit/audit.log
```

```
[vmanaeva@vmanaeva ~]$ sudo tail /var/log/messages
Oct 14 14:56:40 vmanaeva setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 9855aefb-a7c6-4286-bcd5-73265f5aa3be
Oct 14 14:56:48 vmanaeva python: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#0120#012# Plugin restorecon (92.2 confidence) suggests:
21f you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120#012# /bin/restorecon -v /var/www/html/test.html#0120#012# Plugin public_content (7.83 confidence) suggests:
*****#0120#012# If you want to treat test.html as public content#012Then you need to change the label on test.html to public content_t or public content_rw_t.#0120#012# semanage fcontext -a -t public
content_t '/var/www/html/test.html' #012# restorecon -v /var/www/html/test.html #0120#012# Plugin catchall (1.41 confidence) suggests:
*****#0120#012# If you believe that httpd should be
allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120#012# allow this access for now by executing#
#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Oct 14 14:56:42 vmanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 14:56:42 vmanaeva setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#0120#012# Plugin restorecon (92.2 confidence) suggests:
*****#0120#012# If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120#012# /bin/restorecon -v /var/www/html/test.html#0120#012# Plugin public_content (7.83 confidence) suggests:
*****#0120#012# If you want to treat test.html as public content#012Then you need to change the label on test.html to public content_t or public content_rw_t.#0120#012# semanage fcontext -a -t public
content_t '/var/www/html/test.html' #012# restorecon -v /var/www/html/test.html #0120#012# Plugin catchall (1.41 confidence) suggests:
*****#0120#012# If you believe that httpd should be
allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120#012# allow this access for now by executing#
#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Oct 14 14:56:54 vmanaeva dbus[701]: (system) Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Oct 14 14:56:55 vmanaeva dbus[701]: (system) Successfully activated service 'org.fedoraproject.Setroubleshootd'
Oct 14 14:56:55 vmanaeva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 14:56:55 vmanaeva setroubleshoot: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#0120#012# Plugin restorecon (92.2 confidence) suggests:
*****#0120#012# If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to
access a parent directory in which case try to change the following command accordingly.#0120#012# /bin/restorecon -v /var/www/html/test.html#0120#012# Plugin public_content (7.83 confidence) suggests:
*****#0120#012# If you want to treat test.html as public content#012Then you need to change the label on test.html to public content_t or public content_rw_t.#0120#012# semanage fcontext -a -t public
content_t '/var/www/html/test.html' #012# restorecon -v /var/www/html/test.html #0120#012# Plugin catchall (1.41 confidence) suggests:
*****#0120#012# If you believe that httpd should be
allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120#012# allow this access for now by executing#
#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
```

```
[vmanaeva@vmanaeva ~]$ sudo tail /var/
tail: невозможно открыть «/var/log/http/
[vmanaeva@vmanaeva ~]$
```

```
[vmanaeva@vmanaeva ~]$ sudo tail /var/log/http/access_log
tail: невозможно открыть «/var/log/http/access_log» для чтения: Нет такого файла или каталога
[vmanaeva@vmanaeva ~]$
```

```
[vmanaeva@vmanaeva ~]$ sudo tail /var/log/audit/audit.log
type=USER ACCT msg=audit(1697284769.009:634): pid=4795 uid=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER CMD msg=audit(1697284769.009:635): pid=4795 uid=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=CHD PERM msg=audit(1697284769.009:636): pid=4795 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER START msg=audit(1697284769.009:637): pid=4795 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER END msg=audit(1697284769.009:638): pid=4795 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=CHD DISP msg=audit(1697284769.009:639): pid=4795 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=CHD PERM msg=audit(1697284769.009:640): pid=4804 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER ACCT msg=audit(1697284788.355:641): pid=4804 uid=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER CMD msg=audit(1697284788.355:642): pid=4804 uid=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER START msg=audit(1697284788.355:643): pid=4804 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
type=USER END msg=audit(1697284788.355:644): pid=4804 uid=0 audit=1000 ses=1 subj=unconfined_u:unlabeled:object_r:default_t:s0 path=/usr/bin/sudo exe="/usr/bin/sudo" hostname=addr=7 terminal=/dev/pts/8 res=success
[vmanaeva@vmanaeva ~]$
```

19. Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов. Убедимся, что порт 81 появился в списке. (4.18)

```
sudo semanage port -a -t http_port_t --proto tcp 81
semanage port -l | grep http_port_t
```

```
[vmanaeva@vmanaeva ~]$ sudo semanage port -a -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 уже определен
[vmanaeva@vmanaeva ~]$ ^C
[vmanaeva@vmanaeva ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[vmanaeva@vmanaeva ~]$ sudo 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
```

Рис. 4.18: Список портов

20. Пробуем запустить веб-сервер Apache ещё раз. И он работает. (4.19)

```
sudo systemctl start httpd
```

```
[vemanaeva@vemanaeva ~]$ sudo systemctl start httpd
[sudo] пароль для vemanaeva:
Попробуйте ещё раз.
[sudo] пароль для vemanaeva:
[vemanaeva@vemanaeva ~]$
```

Рис. 4.19: Веб-сервер работает

21. Вернём контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. (4.20)

```
chcon -t httpd_sys_content_t /var/www/html/test.html
```

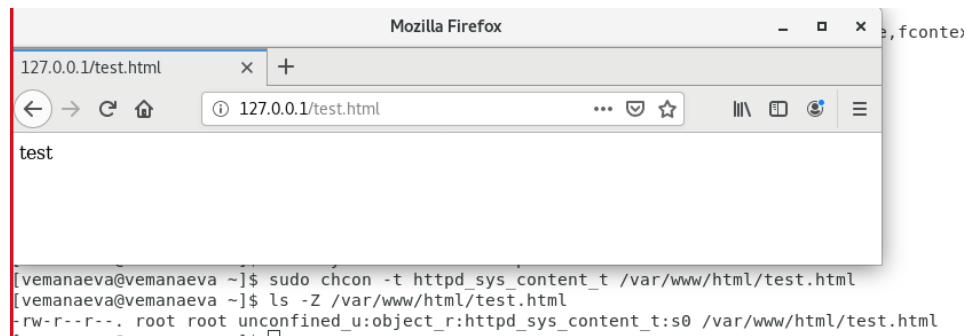


Рис. 4.20: `http://127.0.0.1:81/test.html`

22. Исправим обратно конфигурационный файл `apache`, вернув `Listen 80`. (4.21)

```
nano /etc/httpd/httpd.conf
```

```
GNU nano 2.3.1                                Файл: /etc/httpd/httpd.conf
ServerName test.ru
Listen 80
```

Рис. 4.21: Исправляем конфигурационный файл

23. Удалим привязку `http_port_t` к 81 порту и проверим, что порт 81 удалён. (4.22)

```
semanage port -d -t http_port_t -p tcp 81
```

```
[vemanaeva@vemanaeva ~]$ sudo semanage port -d -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[vemanaeva@vemanaeva ~]$ sudo systemctl start httpd
[vemanaeva@vemanaeva ~]$ sudo semanage port -d -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[vemanaeva@vemanaeva ~]$ █
```

Рис. 4.22: Удаляем привязку

24. Удалим файл /var/www/html/test.html командой (4.23)

```
rm /var/www/html/test.html
```

```
[vemanaeva@vemanaeva ~]$ sudo rm /var/www/html/test.html
[vemanaeva@vemanaeva ~]$ ls -l /var/www/html
итого 0
[vemanaeva@vemanaeva ~]$
```

Рис. 4.23: Удаляем файл

5 Выводы по проделанной работе

5.1 Вывод

В результате выполнения работы мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinux на практике совместно с веб-сервером Apache.

Были записаны скринкасты выполнения и защиты лабораторной работы.

Ссылки на скринкасты:

- Выполнение, Youtube
- Выполнение, Rutube
- Защита презентации, Youtube
- Защита презентации, Rutube

6 Список литературы

1. Лабораторная работа № 6 [Электронный ресурс]. Российский Университет Дружбы Народов имени Патрису Лумумбы, 2023. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031379>.