Отчёт по лабораторной работе 6

Простейший вариант

Еленга Невлора Люглеш

Содержание

1 Цель работы 1
2 Алтуальность 1
3 Выполнение лабораторной работы 1
4 Вывод 8

1 Цель работы

Развить навыки администрирования OCLinux.Получить первое практическое знакомствос технологией SELinux1. Проверить работу SELinx напрактике совместно с веб-сервером Apache.

2 Алтуальность

Веб-сервер Apache – это программное обеспечение, которое установлено на сам сервер. Как мы уже поняли, благодаря ему устанавливается соединение между юзером, использующим браузер, и сервером, чтобы осуществить передачу данных при запросе. Пользователь переходит на страницу, далее отправляется сигнал на обработку, Apache находит необходимые данные и возвращает их пользователю, чтобы тот смог ознакомиться с ними.

3 Выполнение лабораторной работы

1.Вошли в систему с полученными учётными данными и убедились,что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

2.Обратились с помощью браузера к веб-серверу,запущенному на вашем компьютере,иубедитесь,что последний работает: service httpd status или /etc/rc.d/init.d/httpdstatus

Рис. 1.1.

3.Нашли веб-сервер Apache в списке процессов,определите его контекст безопасности изанесите эту информацию в отчёт.Например,можно использовать команду

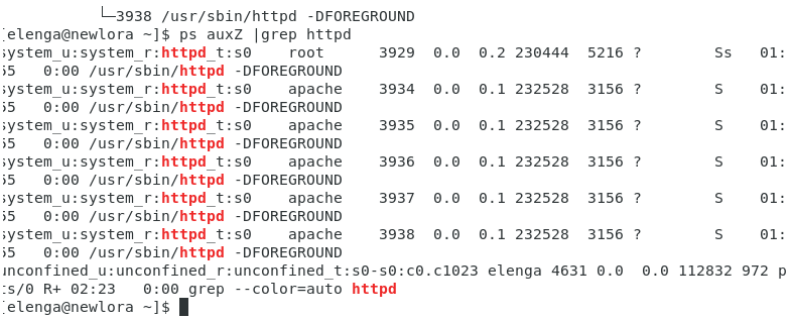

Рис. 1.2.

4.Посмотрули текущее состояние переключателей SELinux для Apachec помощью команды sestatus-bigrep httpd Многие из них находятся вположении «off».

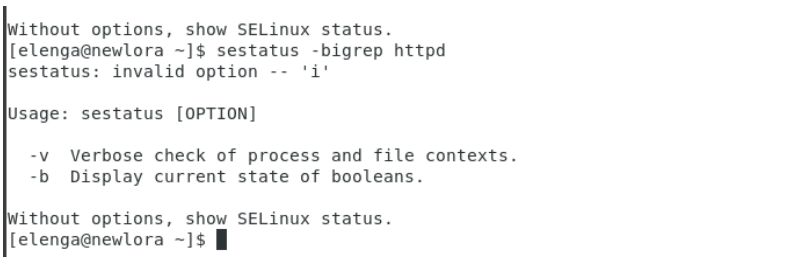

Рис. 1.3.

5.Посмотрули статистику пополитике с помощью команды seinfo,также определите множество пользователей,ролей,типов.

6.Определили тип файлов и поддиректорий,находящихся в директории /var/www,с помощью команды

7.Определили тип файлов,находящихся в директории/var/www/html: ls-lZ/var/www/html

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

Рис. 1.4.

8.Определили круг пользователей,которымразрешеносозданиефайловв директории/var/www/html.

9.Создали отимени суперпользователя(так как в дистрибутиве после установки только ему разрешена запись в директорию)html-файл /var/www/html/test.html следующего содержания:

```
ıароль:
Ɔследний вход в систему:Сб окт 14 02:30:53 MSK 2023на pts/0
[root@newlora ~]# sudo vi /var/www/html/test.html
[root@newlora ~]# sudo vi /var/www/html/test.html
[root@newlora ~]#
```

Рис. 1.5.

```
Файл  Правка  Вид  Поиск  Терминал  Справка
<html>
<body>test</body>
</html>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/var/www/html/test.html" 3L, 33C
```

Рис. 1.6.

10.Проверили контекст созданного вами файла.Занесили в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

```
[root@newlora ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@newlora ~]#
```

Рис. 1.7.

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

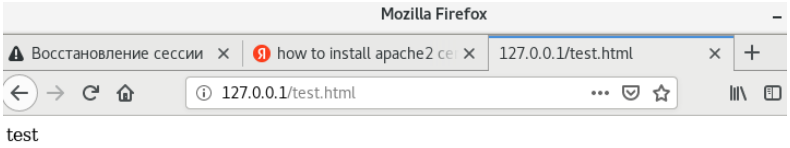

Рис. 1.8.

12.Изучили справку man httpd_selinuxи выясните,какие контексты файлов определены для httpd.Сопоставили их с типом файла test.html.Проверили контекст файла можно командой ls-Z..

13.Изменили контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой,к которому процесс httpd не должен иметь доступа,например,hasamba_share_t:

```
[root@newlora ~]# man httpd_setlinux
Нет справочной страницы для httpd_setlinux
[root@newlora ~]# 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.h
tml
[root@newlora ~]# chcon -t samba_share_t /var/www/html/test.html
[root@newlora ~]# 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@newlora ~]#
```

Рис. 1.9.

14.Попробовали ещё разполучить доступ к файлу через веб-сервер,введяв браузере адрес http://127.0.0.1/test.html.

Получили сообщение обошибке:

Рис. 1.10.

15.Проанализировали ситуацию.Почему файл не был отображён,если права доступа позволяют читать этот файл любому пользователю ls-l/var/www/html/test.html Просмотрите log-файлы веб-сервера Apache.Также просмотрели системный лог-файл:

```
[root@newlora ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 14 02:43 /var/www/html/test.html
[root@newlora ~]# tail /var/log/messages
Oct 14 03:01:29 newlora setroubleshoot: SELinux is preventing httpd from getattr access
 on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 036
88fb1-6cab-4de7-bf22-d8f7e881fcb8
Oct 14 03:01:29 newlora python: SELinux is preventing httpd from getattr access on the
file /var/www/html/test.html.#012#012*****  Plugin restorecon (92.2 confidence) suggest
s   ************************#012#012If you want to fix the label. #012/var/www/html/tes
t.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 paren
```

16.Запустили веб-сервер Apache на прослушивание TCP-порта 81(ане80,как рекомендует IANA и прописанов/etc/services).Для этого в файле/etc/httpd/httpd.conf найдите строчку Listen 80и заменили её на Listen 81.

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81

-- INSERT --
```

Рис. 1.12.

17.Выполнили перезапуск веб-сервера Apache.

```
[root@newlora ~]# sudo systemctl restart httpd
[root@newlora ~]# sudo systemctl sestatus httpd
Unknown operation 'sestatus'.
[root@newlora ~]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disa
bled)
   Active: active (running) since Сб 2023-10-14 03:22:11 MSK; 29s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6191 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 6199 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─6199 /usr/sbin/httpd -DFOREGROUND
           ├─6200 /usr/sbin/httpd -DFOREGROUND
           ├─6201 /usr/sbin/httpd -DFOREGROUND
           ├─6202 /usr/sbin/httpd -DFOREGROUND
           ├─6203 /usr/sbin/httpd -DFOREGROUND
           └─6204 /usr/sbin/httpd -DFOREGROUND

окт 14 03:22:11 newlora.localdomain systemd[1]: Stopped The Apache HTTP Server.
окт 14 03:22:11 newlora.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 03:22:11 newlora.localdomain systemd[1]: Started The Apache HTTP Server.
```

Рис. 1.13.

18.Проанализирули лог-файлы: tail-nl/var/log/messages

```
[root@newlora ~]# tail -n 5 /var/log/audit/audit.log
type=LOGIN msg=audit(1697242201.604:577): pid=5523 uid=0 subj=system_u:system_r:crond_t
:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967295 ses=14 res=1
type=USER_START msg=audit(1697242201.624:578): pid=5523 uid=0 auid=0 ses=14 subj=system
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_loginuid,pam_k
eyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? termi
nal=cron res=success'
type=CRED_REFR msg=audit(1697242201.625:579): pid=5523 uid=0 auid=0 ses=14 subj=system_
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1697242201.667:580): pid=5523 uid=0 auid=0 ses=14 subj=system_
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1697242201.671:581): pid=5523 uid=0 auid=0 ses=14 subj=system_u
:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_ke
yinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? termin
al=cron res=success'
```

Рис. 1.14.

```
[root@newlora ~]# tail -n 10 /var/log/audit/audit.log
type=AVC msg=audit(1697241689.374:574): avc:  denied  { getattr } for  pid=3936 comm="h
ttpd" path="/var/www/html/test.html" dev="dm-0" ino=18306673 scontext=system_u:system_r
:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1697241689.374:574): arch=c000003e syscall=6 success=no exit=-13
 a0=560fb5bdfcb0 a1=7fffae0e7ad0 a2=7fffae0e7ad0 a3=0 items=0 ppid=3929 pid=3936 auid=4
294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) se
s=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(
```

Рис. 1.15.

19.Выполнили команду semanage port-a-thttp_port_t -p tcp 81 После этого проверили список портовкомандой semanage port-l|grep http_port_t

```
[root@newlora ~]# sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@newlora ~]# sudo semanage port -l |grep http_port_t -p tcp 81
grep: неверный ключ — «p»
Использование: grep [ПАРАМЕТР]… ШАБЛОН [ФАЙЛ]…
Запустите «grep --help» для получения более подробного описания.
IOError: [Errno 32] Broken pipe
[root@newlora ~]# 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
[root@newlora ~]#
```

Рис. 1.16.

20.Попробовали запустить веб-сервер Apache ещё раз.

```
[root@newlora ~]# sudo systemctl restart httpd
[root@newlora ~]# sudo systemctl sestatus httpd
Unknown operation 'sestatus'.
[root@newlora ~]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disa
bled)
   Active: active (running) since Сб 2023-10-14 03:22:11 MSK; 29s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6191 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 6199 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─6199 /usr/sbin/httpd -DFOREGROUND
           ├─6200 /usr/sbin/httpd -DFOREGROUND
           ├─6201 /usr/sbin/httpd -DFOREGROUND
           ├─6202 /usr/sbin/httpd -DFOREGROUND
           ├─6203 /usr/sbin/httpd -DFOREGROUND
           └─6204 /usr/sbin/httpd -DFOREGROUND

окт 14 03:22:11 newlora.localdomain systemd[1]: Stopped The Apache HTTP Server.
окт 14 03:22:11 newlora.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 03:22:11 newlora.localdomain systemd[1]: Started The Apache HTTP Server.
```

Рис. 1.17.

21.Вернили контекст httpd_sys_content__t к файлу/var/www/html/test.html: chcon-thttpd_sys_content_t/var/www/html/test.html

После этого попробовали получить доступ к файлу через веб-сервер,введя в браузере адрес http://127.0.0.1:81/test.html. Видели содержимое файла—слово«test».

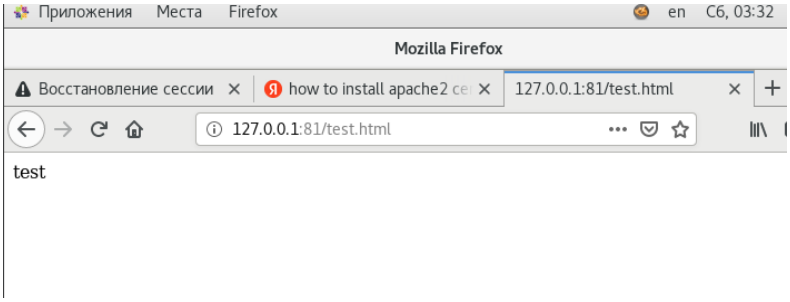

Рис. 1.18.

22.Исправили обратно конфигурационный файла pache,вернув Listen80.

23.Удалили привязку http_port_t к 81 порту: semanage port-d-thttp_port_t-ptcp81 и проверили,что порт 81 удалён.

24.Удалили файли/var/www/html/test.html: rm /var/www/html/test.html

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

Рис. 1.19.

4 Вывод

В ходе выполнения лабораторной работы мы получили первое практическое знакомствос технологией SELinux1. Проверили работу SELinx напрактике совместно с веб-сервером Apache.