

Лабораторная работа №6

Основы информационной безопасности

Феоктистов Владислав Сергеевич

22 сентября 2022

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19

Целью данной работы является:

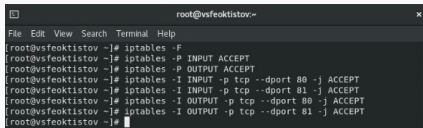
- развитие навыка администрирования ОС Linux;
- получение первого практического знакомства с технологией SELinux;
- проверка работы SELinux на практике совместно с веб-сервером Apache.

- Проверить режим работы и политику SELinux, запустить сервер Apache;
- Создать html-файл test.html и обратиться к нему через веб-сервер;
- Поменять контекст html-файла и поменять порт прослушивания.

Ход выполнения лабораторной работы

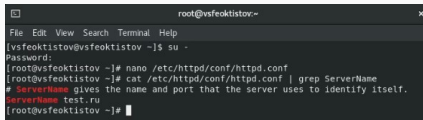
Подготовка лабораторного стенда

Перед выполнением лабораторной работы убедимся, что поддерживается технология SELinux и установлен apache, проверили конфигурационные файлы apache и SELinux, отключили пакетный фильтр и позволили подключаться к 80-у и 81-у портам протокола TCP.



```
root@vsfeoktistov:~  
File Edit View Search Terminal Help  
[root@vsfeoktistov ~]# iptables -F  
[root@vsfeoktistov ~]# iptables -P INPUT ACCEPT  
[root@vsfeoktistov ~]# iptables -P OUTPUT ACCEPT  
[root@vsfeoktistov ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@vsfeoktistov ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@vsfeoktistov ~]# iptables -I OUTPUT -p tcp --dport 80 -j ACCEPT  
[root@vsfeoktistov ~]# iptables -I OUTPUT -p tcp --dport 81 -j ACCEPT  
[root@vsfeoktistov ~]#
```

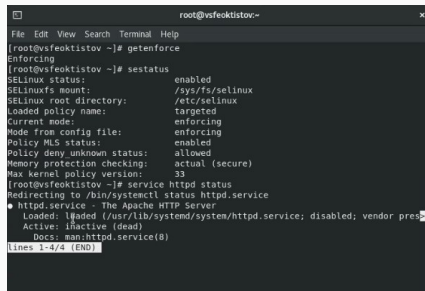
Figure 1: Подготовка лабораторного стенда



```
root@vsfeoktistov:~  
File Edit View Search Terminal Help  
[vsfeoktistov@vsfeoktistov ~]$ su -  
Password:  
[root@vsfeoktistov ~]# nano /etc/httpd/conf/httpd.conf  
[root@vsfeoktistov ~]# cat /etc/httpd/conf/httpd.conf | grep ServerName  
# ServerName gives the name and port that the server uses to identify itself.  
ServerName test.ru  
[root@vsfeoktistov ~]#
```

Figure 2: Подготовка лабораторного стенда

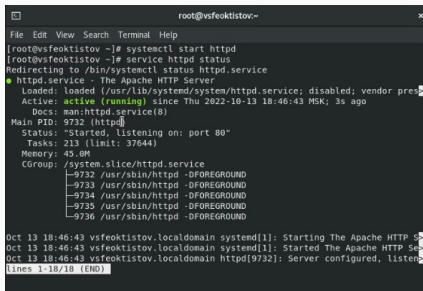
В первую очередь убедимся, что SELinux работает в режиме *enforcing* политики *targeted* с помощью команд *getenforce* и *sestatus*.

A terminal window titled 'root@vsfeoktistov:~' showing the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' shows SELinux is enabled, in enforcing mode, with the targeted policy. The output of 'service httpd status' shows the httpd.service is inactive (dead).

```
root@vsfeoktistov:~  
File Edit View Search Terminal Help  
[root@vsfeoktistov ~]# getenforce  
Enforcing  
[root@vsfeoktistov ~]# 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  
[root@vsfeoktistov ~]# 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: enabled)  
   Active: inactive (dead)  
   Docs: man:httpd.service(8)  
lines 1-4/4 (END)
```

Figure 3: Режим и политика SELinux

С помощью команды `service httpd status` проверили статус работы Apache.

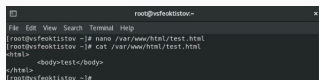


```
root@vsfeoktistov:~  
File Edit View Search Terminal Help  
[root@vsfeoktistov ~]# systemctl start httpd  
[root@vsfeoktistov ~]# service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)  
   Active: active (running) since Thu 2022-10-13 18:46:43 MSK; 3s ago  
     Docs: man:httpd.service(8)  
  Main PID: 9732 (httpd)  
    Status: "Started, listening on: port 80"  
   Tasks: 213 (limit: 37644)  
  Memory: 45.0M  
    CGroup: /system.slice/httpd.service  
            └─9732 /usr/sbin/httpd -DFOREGROUND  
              └─9733 /usr/sbin/httpd -DFOREGROUND  
                └─9734 /usr/sbin/httpd -DFOREGROUND  
                  └─9735 /usr/sbin/httpd -DFOREGROUND  
                    └─9736 /usr/sbin/httpd -DFOREGROUND  
  
Oct 13 18:46:43 vsfeoktistov.localdomain systemd[1]: Starting The Apache HTTP Server:   
Oct 13 18:46:43 vsfeoktistov.localdomain systemd[1]: Started The Apache HTTP Server:   
Oct 13 18:46:43 vsfeoktistov.localdomain httpd[9732]: Server configured, listening on   
lines 1-18/18 (END)
```

Figure 4: Проверка статуса работы Apache

Создание html-файла и обращение к нему через браузер

- Через root-пользователя в каталоге `/var/www/html/` создали html-файл `test.html` и записали в нем простейшую структуру веб-страницы;
- Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.



```
root@vsfeoklistov~#  
File Edit View Search Terminal Help  
[root@vsfeoklistov ~]# nano /var/www/html/test.html  
[root@vsfeoklistov ~]# cat /var/www/html/test.html  
<html>  
  <body>test</body>  
</html>  
[root@vsfeoklistov ~]#
```

Figure 5: Создание html-файла

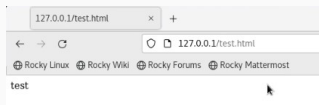


Figure 6: Просмотр файла в веб-браузере

Смена контекста html-файла

- Поменяли контекст html-файла *test.html* командой *chcon* с *httpd_sys_content_t* на *samba_share_t*;
- Перезагрузили веб-страницу и получили сообщение об отказе доступа;
- Посмотри лог-файлы.

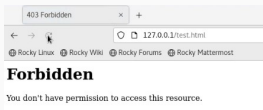


Figure 7: Перезапуск веб-страницы с новым контекстом безопасности *test.html*

```
[root@vsefextstov ~]# ls -l /var/log/httpd
total 8
-rw-r--r-- 1 root root 833 Oct 13 18:28 access.log
-rw-r--r-- 1 root root 1121 Oct 13 18:28 error.log
[root@vsefextstov ~]# tail /var/log/httpd/error.log
[Thu Oct 13 18:46:43.649357 2022] [core:notice] [pid 9732:tid 139781220981824] 0
B:linux policy enabled: httpd running as context system_u:system_r:httpd_t:s0
[Thu Oct 13 18:46:43.652319 2022] [suexec:notice] [pid 9732:tid 139781220981824]
AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Thu Oct 13 18:46:43.703805 2022] [lua:notice] [pid 9732:tid 1397
81220981824] AH02282: No slotown from mod_lua:monitor
[Thu Oct 13 18:46:43.704864 2022] [http:warn] [pid 9732:tid 139781220981824] AH
00923: mod_ssl does not seem to be enabled
[Thu Oct 13 18:46:43.715325 2022] [mpm:event:notice] [pid 9732:tid 1397812209818
24] AH00489: Apache/2.4.37 (rocky) configured -- resuming normal operations
[Thu Oct 13 18:46:43.715331 2022] [core:notice] [pid 9732:tid 139781220981824] A
H00994: command line '/usr/sbin/httpd -D FPM@ONLINE'
[Thu Oct 13 18:28:49.808264 2022] [core:error] [pid 9734:tid 139780197127836] (1)
[1]Permission denied: (client 127.0.0.1:58992) AH00035: access to /test.html deny
ed (filesystem path '/var/www/html/test.html') because search permissions are mi
ssing on a component of the path
[root@vsefextstov ~]#
```

Figure 8: Просмотр лог-файла

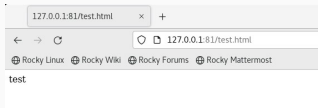
Установка порта прослушивания и возвращение контекста безопасности

- В конфигурационном файле `/etc/httpd/conf/httpd.conf` установили 81 порт прослушивания;
- С помощью команды `semanage` добавили этот порт в список прослушиваемых портов и проверили его добавление;
- Перезапустили Apache, вернули контекст `httpd_sys_content_t` файлу `test.html` и зашли на веб-страницу под 81 портом.

```
root@vsfeaktistov~  
File Edit View Search Terminal Help  
[root@vsfeaktistov ~]# nano /etc/httpd/conf/httpd.conf  
[root@vsfeaktistov ~]# cat /etc/httpd/conf/httpd.conf | grep Listen  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# Change this to Listen on specific IP addresses as shown below to  
# Listen 12.34.56.78:80  
Listen 81  
[root@vsfeaktistov ~]# systemctl restart httpd  
[root@vsfeaktistov ~]#
```

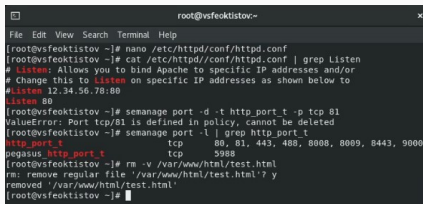
```
root@vsfeaktistov~  
File Edit View Search Terminal Help  
[root@vsfeaktistov ~]# semanage port -a -t http_port_t -p tcp 81  
valueError: Port tcp/81 already defined  
[root@vsfeaktistov ~]# semanage port -l | grep http_port_t  
http_port_t      tcp      80, 81  443, 488, 8080, 8089, 8443, 9000  
pegasus_http_port_t tcp      5988  
[root@vsfeaktistov ~]# systemctl restart httpd
```

```
root@vsfeaktistov~  
File Edit View Search Terminal Help  
[root@vsfeaktistov ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@vsfeaktistov ~]# ls -lZ /var/www/html/test.html  
-rw-r--r-- 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 13 1  
8:57 /var/www/html/test.html  
[root@vsfeaktistov ~]#
```



Возвращение стандартных настроек

Перед завершением работы, исправили конфигурационный файл Apache, вернув *Listen 80*, удалили привязку *http_port* к 81 порту и удалили файл */var/www/html/test.html*.



```
root@vsfeoktistov:~  
File Edit View Search Terminal Help  
[root@vsfeoktistov ~]# nano /etc/httpd/conf/httpd.conf  
[root@vsfeoktistov ~]# cat /etc/httpd/conf/httpd.conf | grep Listen  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# Change this to Listen on specific IP addresses as shown below to  
#Listen 12.34.56.78:80  
Listen 80  
[root@vsfeoktistov ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted  
[root@vsfeoktistov ~]# 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@vsfeoktistov ~]# rm -v /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'? y  
removed '/var/www/html/test.html'  
[root@vsfeoktistov ~]#
```

Figure 9: Возвращение стандартных настроек

В процессе выполнения лабораторной работы:

- развил навыки администрирования ОС Linux;
- получил первое практическое знакомство с технологией SELinux;
- проверил работу SELinux на практике совместно с веб-сервером Apache.