

# **Отчёт по лабораторной работе №6**

## **Знакомство с SELinux**

Альсид Мона НФИбд-03-18

## Содержание

1	Цель работы .....	3
2	Выполнение лабораторной работы.....	4
2.1	Подготовка .....	4
2.2	Изучение механики SetUID.....	4
3	Выводы.....	9

## **1      Цель работы**

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

## 2 Выполнение лабораторной работы

### 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

### 2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.

```
[root@mona alseedmona]# 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@mona alseedmona]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@mona alseedmona]# 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 Sat 2021-11-27 15:05:26 MSK; 1h 49min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 1420 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─1420 /usr/sbin/httpd -DFOREGROUND
              └─1421 /usr/sbin/httpd -DFOREGROUND
                └─1422 /usr/sbin/httpd -DFOREGROUND
                  └─1423 /usr/sbin/httpd -DFOREGROUND
                    └─1424 /usr/sbin/httpd -DFOREGROUND
                      └─1425 /usr/sbin/httpd -DFOREGROUND

Nov 27 15:05:16 mona.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 27 15:05:21 mona.localdomain httpd[1420]: AH00558: httpd: Could not reliably determine the...age
Nov 27 15:05:26 mona.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@mona alseedmona]#
```

Figure 1: запуск http

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

```

[root@mona alseedmona]# 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 Sat 2021-11-27 15:05:26 MSK; 1h 49min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 1420 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─1420 /usr/sbin/httpd -DFOREGROUND
              └─1421 /usr/sbin/httpd -DFOREGROUND
                └─1422 /usr/sbin/httpd -DFOREGROUND
                  └─1423 /usr/sbin/httpd -DFOREGROUND
                    └─1424 /usr/sbin/httpd -DFOREGROUND
                      └─1425 /usr/sbin/httpd -DFOREGROUND

Nov 27 15:05:16 mona.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 27 15:05:21 mona.localdomain httpd[1420]: AH00558: httpd: Could not reliably determine the...age
Nov 27 15:05:26 mona.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@mona alseedmona]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      1420  0.0  0.5 230440  5204 ?        Ss   15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  1421  0.0  0.2 230440  2992 ?        S    15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  1422  0.0  0.2 230440  2992 ?        S    15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  1423  0.0  0.2 230440  2992 ?        S    15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  1424  0.0  0.2 230440  2992 ?        S    15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  1425  0.0  0.2 230440  2992 ?        S    15:05   0:00 /usr
r/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root  2107  0.0  0.0 112812  980 tty1 S+  17:02
0:00 grep --color=auto httpd
[root@mona alseedmona]# _

```

Figure 2: контекст безопасности http

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».

```

virt_use_comm off
virt_use_execmem off
virt_use_fusefs off
virt_use_glusterd off
virt_use_nfs off
virt_use_rawip off
virt_use_samba off
virt_use_sanlock off
virt_use_usb on
virt_use_xserver off
webadm_manage_user_files off
webadm_read_user_files off
wine_mmap_zero_ignore off
xdm_bind_vnc_tcp_port off
xdm_exec_bootloader off
xdm_sysadm_login off
xdm_write_home off
xen_use_nfs off
xend_run_blkmap on
xend_run_gemu on
xguest_connect_network on
xguest_exec_content on
xguest_mount_media on
xguest_use_bluetooth on
xserver_clients_write_xshm off
xserver_execmem off
xserver_object_manager off
zabbix_can_network off
zabbix_run_sudo off
zarafa_setrlimit off
zebra_write_config off
zoneminder_anon_write off
zoneminder_run_sudo off
[guest@mona alseedmona]$ 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
[guest@mona alseedmona]$ ls -lZ /var

```

Figure 3: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы может только root.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания: Test
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.

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

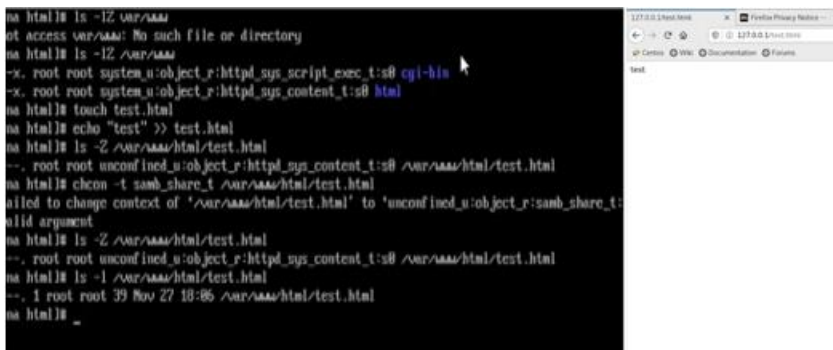


Figure 4: создание html-файла и доступ по http

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
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, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.
14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.` При изменении контекста файл стал считаться чужим для `http` и программа не может его прочитать.

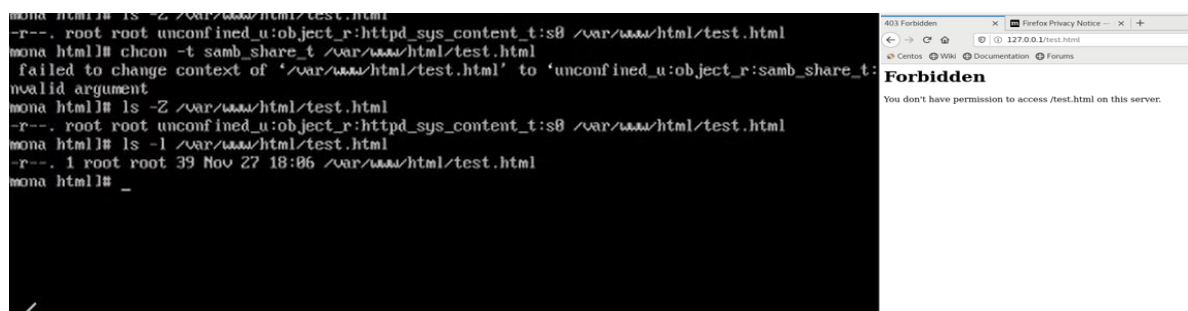


Figure 5: ошибка доступа после изменения контекста

15. Проанализируйте 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

просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

16. Попробуйте запустить 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`.
17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.
19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз.
21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».

```
[root@mona html]# 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@mona html]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@mona html]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@mona html]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'?
[root@mona html]#
```

Figure 6: доступ по http на 81 порту

22. Исправьте обратно конфигурационный файл apache, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`



### **3      Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.