Лабораторная работа №6

Мандатное разграничение прав в Linux

Латыпова Диана

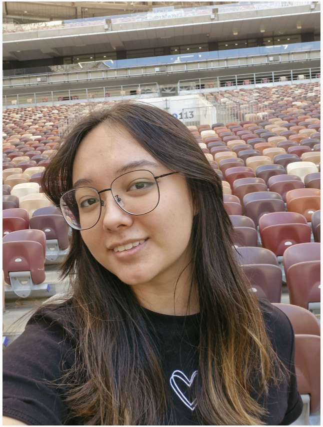
12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Латыпова Диана
- студент группы НФИбд-02-21
- Российский университет дружбы народов
- 1032215005@rudn.ru
- https://github.com/dlatypova



Вводная часть

Цели и задачи

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

Теоретическая справка

SELinux (Security-Enhanced Linux)

- система управления доступом на уровне ядра, которая реализует обязательное управление доступом (MAC) в операционных системах Linux.

Использует три режима работы:

- Enforcing
- Permissive
- Disabled

Команды для управления и проверки статуса:

- getenforce
- sestatus

Apache

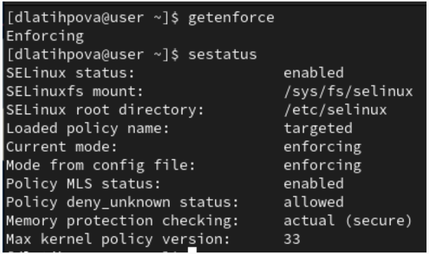
- один из самых популярных веб-серверов, который используется для обслуживания веб-сайтов и приложений

При работе с веб-сервером и SELinux важно отслеживать логи:

- /var/log/messages
- /var/log/httpd/error_log
- /var/log/audit/audit.log

Выполнение лабораторной работы

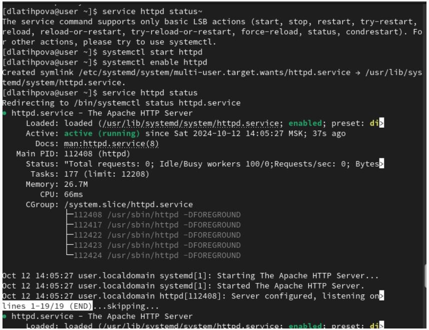
Командыgetenforce и sestatus



```
[dlatihpova@user ~]$ getenforce
Enforcing
[dlatihpova@user ~]$ 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
```

Рис. 1: Пункт 1

service httpd status

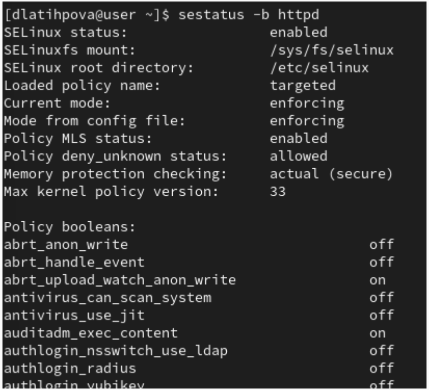


```
[dlatihpova@user ~]$ service httpd status~
The service command supports only basic LSB actions (start, stop, restart, try-restart,
reload, reload-or-restart, try-reload-or-restart, force-reload, status, condrestart). Fo
r other actions, please try to use systemctl.
[dlatihpova@user ~]$ systemctl start httpd
[dlatihpova@user ~]$ systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/sys
temd/system/httpd.service.
[dlatihpova@user ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
     Active: active (running) since Sat 2024-10-12 14:05:27 MSK; 37s ago
       Docs: man:httpd.service(8)
   Main PID: 112408 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
      Tasks: 177 (limit: 12208)
     Memory: 26.7M
        CPU: 66ms
     CGroup: /system.slice/httpd.service
             ├─112408 /usr/sbin/httpd -DFOREGROUND
             ├─112417 /usr/sbin/httpd -DFOREGROUND
             ├─112422 /usr/sbin/httpd -DFOREGROUND
             ├─112423 /usr/sbin/httpd -DFOREGROUND
             └─112424 /usr/sbin/httpd -DFOREGROUND

Oct 12 14:05:27 user.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 12 14:05:27 user.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 12 14:05:27 user.localdomain httpd[112408]: Server configured, listening on>
lines 1-19/19 (END)...skipping...
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di>
```

Рис. 2: Пункт 2

Текущее состояние переключателей SELinux для Apache

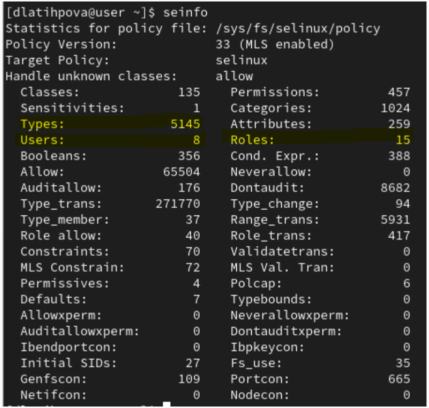


```
[dlatihpova@user ~]$ sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

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
```

Рис. 3: Пункт 4

Поросмотр статистики по политике

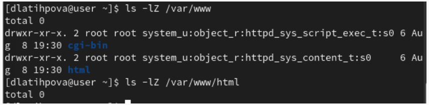


```
[dlatihpova@user ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:         457
  Sensitivities:         1    Categories:         1024
  Types:              5145    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            356    Cond. Expr.:         388
  Allow:             65504    Neverallow:            0
  Auditallow:          176    Dontaudit:          8682
  Type_trans:       271770    Type_change:          94
  Type_member:          37    Range_trans:        5931
  Role allow:           40    Role_trans:          417
  Constraints:          70    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           4    Polcap:                6
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               35
  Genfscon:            109    Portcon:             665
  Netifcon:              0    Nodecon:               0
```

Рис. 4: Пункт 5

Команда `ls -Z`

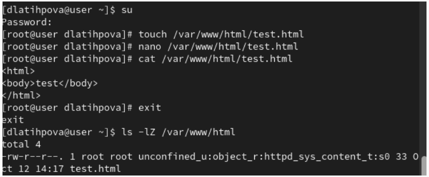
- `ls -Z /var/www/html/test.html` — показывает контекст безопасности файла



```
[dlatihpova@user ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Au
g  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 Au
g  8 19:30 html
[dlatihpova@user ~]$ ls -lZ /var/www/html
total 0
```

Рис. 5: Пункты 6-8

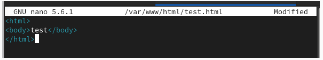
Файл test.html (1)



```
[dlatihpova@user ~]$ su
Password:
[root@user dlatihpova]# touch /var/www/html/test.html
[root@user dlatihpova]# nano /var/www/html/test.html
[root@user dlatihpova]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@user dlatihpova]# exit
exit
[dlatihpova@user ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 O
ct 12 14:17 test.html
```

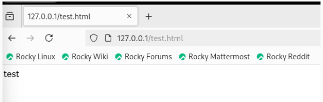
Рис. 6: Пункты 9-10

Файл test.html (2)



```
  GNU nano 5.6.1              /var/www/html/test.html              Modified
<html>
<body>test</body>
</html>
```

Рис. 7: Содержимое файла test.html

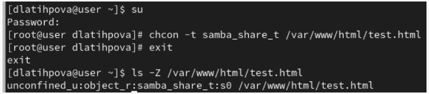


test

Рис. 8: Пункт 11

Команда chcon

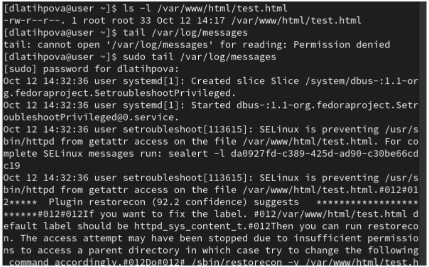
- `chcon -t` — изменяет тип контекста



```
[dlatihpova@user ~]$ su
Password:
[root@user dlatihpova]# chcon -t samba_share_t /var/www/html/test.html
[root@user dlatihpova]# exit
exit
[dlatihpova@user ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 9: Пункт 13

Просмотр log-файлов веб-сервера Apache

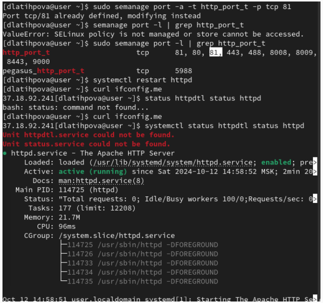


```
[dlatihpova@user ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 12 14:17 /var/www/html/test.html
[dlatihpova@user ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[dlatihpova@user ~]$ sudo tail /var/log/messages
[sudo] password for dlatihpova:
Oct 12 14:32:36 user systemd[1]: Created slice Slice /system/dbus-:1.1-or
g.fedoraproject.SetroubleshootPrivileged.
Oct 12 14:32:36 user systemd[1]: Started dbus-:1.1-org.fedoraproject.Setr
oubleshootPrivileged@0.service.
Oct 12 14:32:36 user setroubleshoot[113615]: SELinux is preventing /usr/s
bin/httpd from getattr access on the file /var/www/html/test.html. For co
mplete SELinux messages run: sealert -l da0927fd-c389-425d-ad90-c30be66cd
c19
Oct 12 14:32:36 user setroubleshoot[113615]: SELinux is preventing /usr/s
bin/httpd from getattr access on the file /var/www/html/test.html.#012#01
2*****  Plugin restorecon (92.2 confidence) suggests   ******************
******#012#012If you want to fix the label. #012/var/www/html/test.html d
efault label should be httpd_sys_content_t.#012Then you can run restoreco
n. The access attempt may have been stopped due to insufficient permissio
ns to access a parent directory in which case try to change the following
 command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.h
```

Рис. 10: Пункт 15

Работа с портами

- `semanage port -a -t` — добавляет порт к списку допустимых для Apache
- `semanage port -l | grep http_port_t` - просмотр списка портов, разрешённых SELinux
- `semanage port -d -t http_port_t -p` - удаляет привязку порта



```
[dlatihpova@user ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[dlatihpova@user ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[dlatihpova@user ~]$ sudo semanage port -l | grep http_port_t
http_port_t                    tcp      81, 80, 81, 443, 488, 8008, 8009,
 8443, 9000
pegasus_http_port_t            tcp      5988
[dlatihpova@user ~]$ systemctl restart httpd
[dlatihpova@user ~]$ curl ifconfig.me
37.18.92.241[dlatihpova@user ~]$ status httpdtl status httpd
bash: status: command not found...
[dlatihpova@user ~]$ curl ifconfig.me
37.18.92.241[dlatihpova@user ~]$ systemctl status httpdtl status httpd
Unit httpdtl.service could not be found.
Unit status.service could not be found.
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; pre>
     Active: active (running) since Sat 2024-10-12 14:58:52 MSK; 2min 20>
       Docs: man:httpd.service(8)
   Main PID: 114725 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0>
      Tasks: 177 (limit: 12208)
     Memory: 21.7M
        CPU: 96ms
     CGroup: /system.slice/httpd.service
             ├─114725 /usr/sbin/httpd -DFOREGROUND
             ├─114726 /usr/sbin/httpd -DFOREGROUND
             ├─114733 /usr/sbin/httpd -DFOREGROUND
             ├─114734 /usr/sbin/httpd -DFOREGROUND
             └─114735 /usr/sbin/httpd -DFOREGROUND

Oct 12 14:58:51 user.localdomain systemd[1]: Starting The Apache HTTP Se>
```

Рис. 11: Пункты 19-20

Выводы

Выводы

- Развиты навыки администрирования ОС Linux
- Получено первое практическое знакомство с технологией SELinux
- Проверена работа SELinx на практике совместно с веб-сервером Apache