Презентация по лабораторной работе №6

Информационная безопасность

Чекалова Л. Р.

12 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Чекалова Лилия Руслановна
- студент 4 курса группы НФИбд-02-20
- ст. б. 1032201654
- Российский университет дружбы народов
- 1032201654@pfur.ru

Вводная часть

Цели и задачи

- Приобретение навыков администрирования в Linux
- Изучение SELinux и веб-сервера Apache
- Работа с лог-файлами

Материалы и методы

- Веб-сервис `GitHub` для работы с репозиториями
- Программа для виртуализации ОС `VirtualBox`
- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `docx`
- Автоматизация процесса создания: `Makefile`

Ход работы

Проверка режима работы SELinux

```
[lrchekalova@lrchekalova ~]$ getenforce
Enforcing
[lrchekalova@lrchekalova ~]$ 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
[lrchekalova@lrchekalova ~]$
```

Запуск веб-сервера

```
[lrchekalova@lrchekalova ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[lrchekalova@lrchekalova ~]$ 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; preset: disabled)
     Active: active (running) since Thu 2023-10-12 13:30:27 MSK; 15s ago
       Docs: man:httpd.service(8)
   Main PID: 3985 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 213 (limit: 12143)
     Memory: 29.4M
        CPU: 180ms
     CGroup: /system.slice/httpd.service
             ├─3985 /usr/sbin/httpd -DFOREGROUND
             ├─3993 /usr/sbin/httpd -DFOREGROUND
             ├─3995 /usr/sbin/httpd -DFOREGROUND
             ├─3999 /usr/sbin/httpd -DFOREGROUND
             └─4000 /usr/sbin/httpd -DFOREGROUND
[lrchekalova@lrchekalova ~]$
```

Просмотр контекста процесса веб-сервера

```
[lrchekalova@lrchekalova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        3985  0.0  0.5  20328 11720 ?        Ss   13:30
 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      3993  0.0  0.3  21664  7600 ?        S    13:30
 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      3995  0.0  0.7 1210612 15280 ?       Sl   13:30
 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      3999  0.0  0.6 1079476 13228 ?       Sl   13:30
 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      4000  0.0  0.6 1079476 13232 ?       Sl   13:30
 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 lrcheka+ 4258 0.0  0.1 221688 2420 pts/
0 S+ 13:32   0:00 grep --color=auto httpd
[lrchekalova@lrchekalova ~]$
```

Просмотр статистики по политике

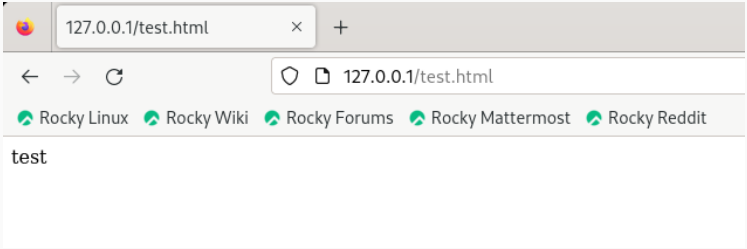
```
[lrchekalova@lrchekalova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             135    Permissions:          457
  Sensitivities:         1    Categories:          1024
  Types:              5100    Attributes:           258
  Users:                 8    Roles:                 14
  Booleans:            353    Cond. Expr.:          384
  Allow:             65008    Neverallow:             0
  Auditallow:          170    Dontaudit:           8572
  Type_trans:       265344    Type_change:           87
  Type_member:          35    Range_trans:         6164
  Role allow:           38    Role_trans:           420
  Constraints:          70    Validatetrans:          0
  MLS Constrain:        72    MLS Val. Tran:          0
  Permissives:           2    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:              660
  Netifcon:              0    Nodecon:                0
[lrchekalova@lrchekalova ~]$ seinfo -t

Types: 5100
   NetworkManager_dispatcher_chronyc_script_t
```

Просмотр контекстов папок и создание Html-файла

```
[lrchekalova@lrchekalova ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 мая 16 23:21 html
[lrchekalova@lrchekalova ~]$ ls -lZ /var/www/html
итого 0
[lrchekalova@lrchekalova ~]$
```

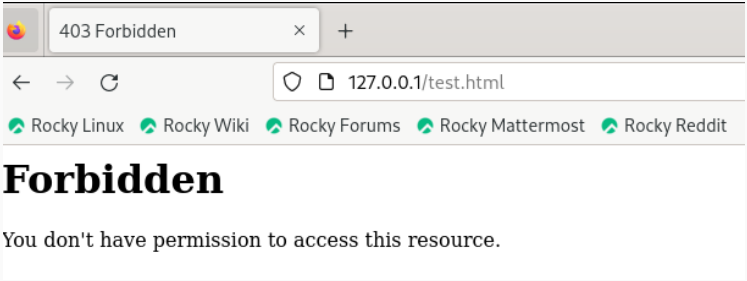
```
[lrchekalova@lrchekalova ~]$ su
Пароль:
[root@lrchekalova lrchekalova]# touch /var/www/html/test.html
[root@lrchekalova lrchekalova]# echo '<html>' > /var/www/html/test.html
[root@lrchekalova lrchekalova]# echo '<body>test</body>' >> /var/www/html/test.html
[root@lrchekalova lrchekalova]# echo '</html>' >> /var/www/html/test.html
[root@lrchekalova lrchekalova]#
```

Отображение файла в браузере



Изменение контекста и просмотр файла в браузере

```
[root@lrchekalova lrchekalova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@lrchekalova lrchekalova]# chcon -t samba_share_t /var/www/html/test.html
[root@lrchekalova lrchekalova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@lrchekalova lrchekalova]#
```



Просмотр лог-файлов

```
[root@lrchekalova lrchekalova]# tail /etc/httpd/logs/access_log
127.0.0.1 - - [12/Oct/2023:13:54:50 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0
(X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [12/Oct/2023:13:54:51 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.
0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [12/Oct/2023:14:03:05 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0
 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Изменение порта и перезапуск сервера

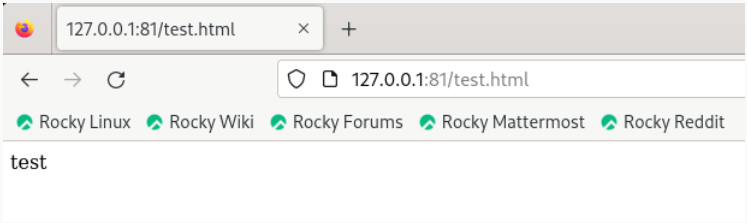
```
[root@lrchekalova conf]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@lrchekalova conf]# cd
[root@lrchekalova ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: active (running) since Thu 2023-10-12 14:27:19 MSK; 2min 9s ago
       Docs: man:httpd.service(8)
   Main PID: 6491 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: >
      Tasks: 213 (limit: 12143)
     Memory: 34.7M
        CPU: 260ms
     CGroup: /system.slice/httpd.service
             ├─6491 /usr/sbin/httpd -DFOREGROUND
             ├─6492 /usr/sbin/httpd -DFOREGROUND
             ├─6496 /usr/sbin/httpd -DFOREGROUND
             ├─6497 /usr/sbin/httpd -DFOREGROUND
             └─6499 /usr/sbin/httpd -DFOREGROUND

окт 12 14:27:19 lrchekalova.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 12 14:27:19 lrchekalova.localdomain systemd[1]: Started The Apache HTTP Server.
окт 12 14:27:19 lrchekalova.localdomain httpd[6491]: Server configured, listening on: port 81
```

Просмотр списка портов

```
[root@lrchekalova ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@lrchekalova ~]# 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@lrchekalova ~]#
```

Возвращение контекста и просмотр в браузере

```
[root@lrchekalova ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@lrchekalova ~]#
```



Удаление порта и файла

```
[root@lrchekalova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@lrchekalova ~]# 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@lrchekalova ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@lrchekalova ~]#
```

Результаты

Результаты работы

- Получены базовые навыки администрирования в Linux
- Рассмотрены принципы работы SELinux
- Изучены принципы работы веб-сервера Apache