Лабораторная работа №6

Информационная безопасность

Николаев Д. И.

8 октября 2023

Российский университет дружбы народов, Москва, Россия

Прагматика выполнения

Прагматика выполнения

- Повышение навыков администрирования ОС Linux;
- Знакомство с технологией SELinux и проверка ее работы на практике совместно с веб-сервером Apache;
- Применение полученных знаний на практике в дальнейшем.

Цели

Цели

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

Задачи

Задачи

1. Ознакомиться с технологией SELinux;
2. Проверить работу SELinux в связке с веб-сервером Apache.

Выполнение работы

Проверка режима работы SELinux

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

Рис. 1: Режим работы SELinux

Обращение к веб-серверу

```
[dinikolaev@dinikolaev ~]$ 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 Sat 2023-10-07 22:32:51 MSK; 2min 12s ago
       Docs: man:httpd.service(8)
   Main PID: 42745 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 213 (limit: 5689)
     Memory: 38.2M
        CPU: 134ms
     CGroup: /system.slice/httpd.service
             ├─42745 /usr/sbin/httpd -DFOREGROUND
             ├─42753 /usr/sbin/httpd -DFOREGROUND
             ├─42754 /usr/sbin/httpd -DFOREGROUND
             ├─42755 /usr/sbin/httpd -DFOREGROUND
             └─42756 /usr/sbin/httpd -DFOREGROUND

окт 07 22:32:51 dinikolaev systemd[1]: Starting The Apache HTTP Server...
окт 07 22:32:51 dinikolaev systemd[1]: Started The Apache HTTP Server.
окт 07 22:32:51 dinikolaev httpd[42745]: Server configured, listening on: port 80
[dinikolaev@dinikolaev ~]$
```

Рис. 2: Обращение к веб-серверу

Проверка контекста безопасности

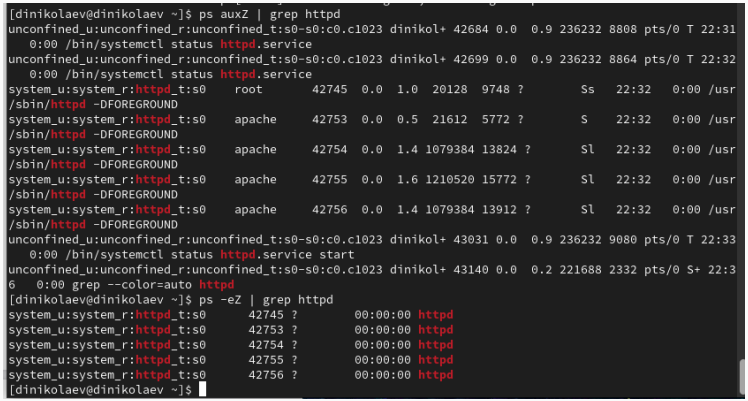

Рис. 3: Проверка контекста безопасности процессов

Статистика по политике

```
[dinikolaev@dinikolaev ~]$ 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:              5135    Attributes:          259
  Users:                 8    Roles:                15
  Booleans:            357    Cond. Expr.:         390
  Allow:             65380    Neverallow:            0
  Auditallow:          172    Dontaudit:          8647
  Type_trans:       267809    Type_change:          94
  Type_member:          37    Range_trans:        6164
  Role allow:           39    Role_trans:          419
  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:             665
  Netifcon:              0    Nodecon:               0
[dinikolaev@dinikolaev ~]$
```

Контекст созданного файла

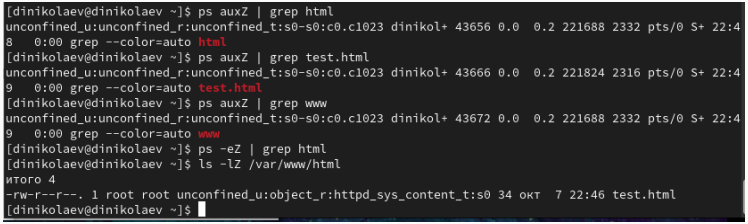

Рис. 5: Проверка контекста созданного файла

Обращение к файлу через браузер

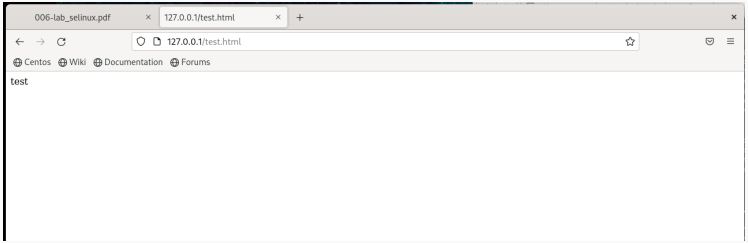

Рис. 6: Обращение к файлу через веб-сервер

Смена контекста файла

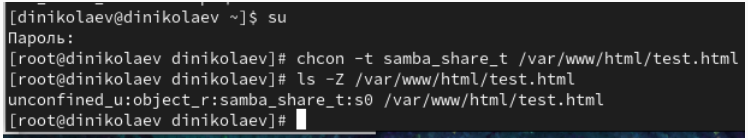

Рис. 7: Смена контекста файла

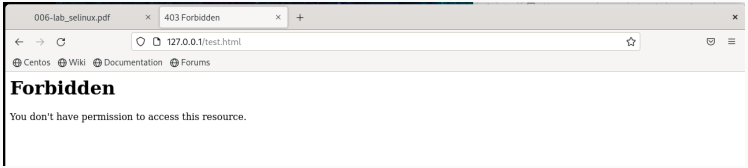

Рис. 8: Попытка получения доступа к файлу через веб-сервер

Сообщения log-файла

```
[dinikolaev@dinikolaev ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[dinikolaev@dinikolaev ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 окт  7 22:46 /var/www/html/test.html
[dinikolaev@dinikolaev ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[dinikolaev@dinikolaev ~]$ sudo tail /var/log/messages
[sudo] пароль для dinikolaev:
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for webkit2gtk3-jsc
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-core
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-modules
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-modules-core
Oct  7 23:11:58 dinikolaev packagekitd[2066]: Failed to get cache filename for kernel-devel
Oct  7 23:12:07 dinikolaev systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service:
Deactivated successfully.
Oct  7 23:12:07 dinikolaev systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct  7 23:14:32 dinikolaev systemd[1]: Starting Fingerprint Authentication Daemon...
Oct  7 23:14:32 dinikolaev systemd[1]: Started Fingerprint Authentication Daemon.
```

Рис. 9: Последние сообщения log-файла

Перезапуск веб-сервера Apache

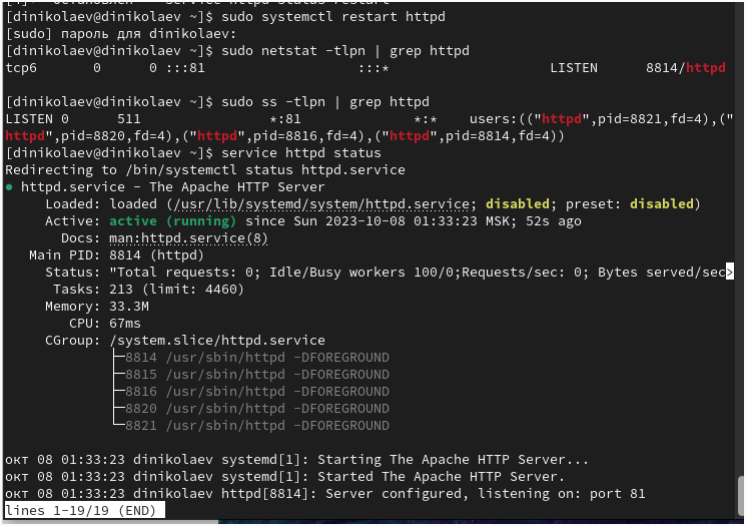

Рис. 10: Перезапуск веб-сервера Apache

Попытка подключения через браузер

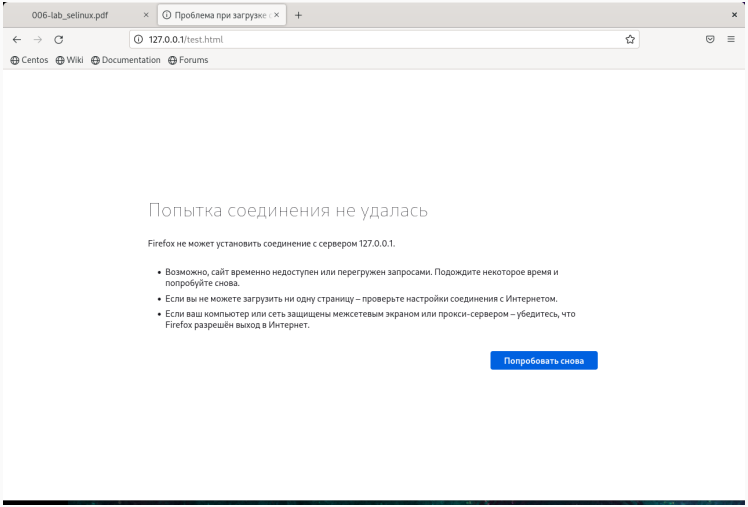

Рис. 11: Попытка подключения к веб-серверу через браузер

Установка 81 порта

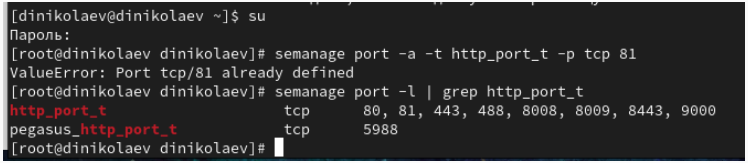

Рис. 12: Установка 81 порта и проверка списка всех портов

Установка 81 порта

```
[dinikolaev@dinikolaev ~]$ su
Пароль:
[root@dinikolaev dinikolaev]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@dinikolaev dinikolaev]#
```

Рис. 13: Возвращение контекста httpd_sys_content_t нашему файлу

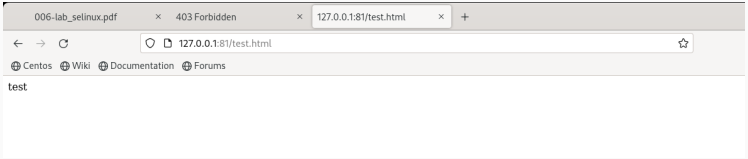

Рис. 14: Получение доступа к файлу через браузер

Попытка удаления привязки к 81 порту

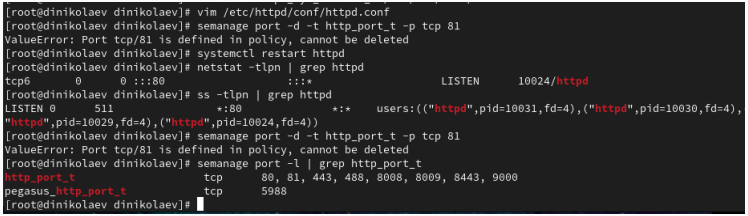

Рис. 15: Попытка удаления привязки к 81 порту

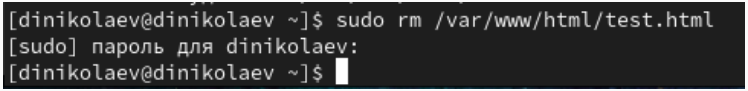

Рис. 16: Удаление файла test.html

Результаты

Результаты

По результатам работы, я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux и проверил работу SELinux на практике совместно с веб-сервером Apache.