

Отчет по лабораторной работе 6

Дисциплина: Информационная безопасность

Хрусталеv Влад Николаевич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	13

Список иллюстраций

2.1	Проверка статуса SeLinux	6
2.2	Проверка статуса httpd	6
2.3	Просмотр контекста безопасности httpd	7
2.4	Текущее состояние переключателей SELinux для Apache	7
2.5	StInfo	7
2.6	Тип файлов и поддиректорий, находящихся в директории /var/www	7
2.7	Тип файлов и поддиректорий, находящихся в директории /var/www/html	8
2.8	Создание html-файл /var/www/html/test.html	8
2.9	Контекст созданного файла	8
2.10	Отображение на сайте	9
2.11	man httpd_selinux	9
2.12	Измените контекст файла /var/www/html/test.html	9
2.13	Отображение на сайте с изменённые контекстом файла	10
2.14	Просмотр логов	10
2.15	Изменение прослушиваемого порта Apache на 81	10
2.16	Перезапуск Apache	11
2.17	Добавление порта 81 в разрешённые	11
2.18	Возврат стандарт контекста	11
2.19	Проверка сайта	11
2.20	Возврат стандартного порта	12
2.21	Попытка отключения порта 81	12

Список таблиц

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

1. Сделаем подготовительные операции перед работой (рис. 2.2 и 2.1)

```
[vnkhrustalev@vnkhrustalev ~]$ 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: disabled)
   Active: active (running) since Sat 2024-04-27 19:46:36 MSK; 15min ago
     Docs: man:httpd.service(8)
   Main PID: 1304 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
   Tasks: 213 (limit: 24609)
   Memory: 33.9M
     CPU: 1.180s
   CGroup: /system.slice/httpd.service
           └─1304 /usr/sbin/httpd -DFOREGROUND
             └─1324 /usr/sbin/httpd -DFOREGROUND
               └─1325 /usr/sbin/httpd -DFOREGROUND
                 └─1326 /usr/sbin/httpd -DFOREGROUND
                   └─1327 /usr/sbin/httpd -DFOREGROUND

anp 27 19:46:34 vnkhrustalev.localdomain systemd[1]: Starting The Apache HTTP Server:
anp 27 19:46:36 vnkhrustalev.localdomain systemd[1]: Started The Apache HTTP Server:
anp 27 19:46:36 vnkhrustalev.localdomain httpd[1304]: Server configured, listening on
```

Рис. 2.1: Проверка статуса SeLinux

```
vnkhrustalev@vnkhrustalev:~$ getenforce
Enforcing
```

Рис. 2.2: Проверка статуса httpd

2. Определение контекста безопасности и попытка проверки наличия команды StInfo. +sestatus команды не существует. (рис. 2.3 и 2.4 и 2.4)

```
[vnkhrustalev@vnkhrustalev ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 1304 0.0 0.2 20328 11588 ?
Ss 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1324 0.0 0.1 21664 7332 ?
S 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1325 0.0 0.3 1669372 15132 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1326 0.0 0.3 1538236 15132 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1327 0.0 0.2 1538236 11044 ?
Sl 19:46 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vnkhrus+ 3314 0.0 0.0 221
320 2340 pts/0 S+ 20:02 0:00 grep --color=auto httpd
[vnkhrustalev@vnkhrustalev ~]$
```

Рис. 2.3: Просмотр контекста безопасности httpd

```
[vnkhrustalev@vnkhrustalev ~]$ 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
awstats_purge_apache_log_files off
```

Рис. 2.4: Текущее состояние переключателей SELinux для Apache

```
[vnkhrustalev@vnkhrustalev ~]$ seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] N

[vnkhrustalev@vnkhrustalev ~]$
```

Рис. 2.5: StInfo

3. Определение типов файлов в директориях Apache (файлов сервера) (рис. 2.6 и 2.7)

```
[vnkhrustalev@vnkhrustalev ~]$ ls -lZ /var/www/html
итого 0
[vnkhrustalev@vnkhrustalev ~]$
```

Рис. 2.6: Тип файлов и поддиректорий, находящихся в директории /var/www

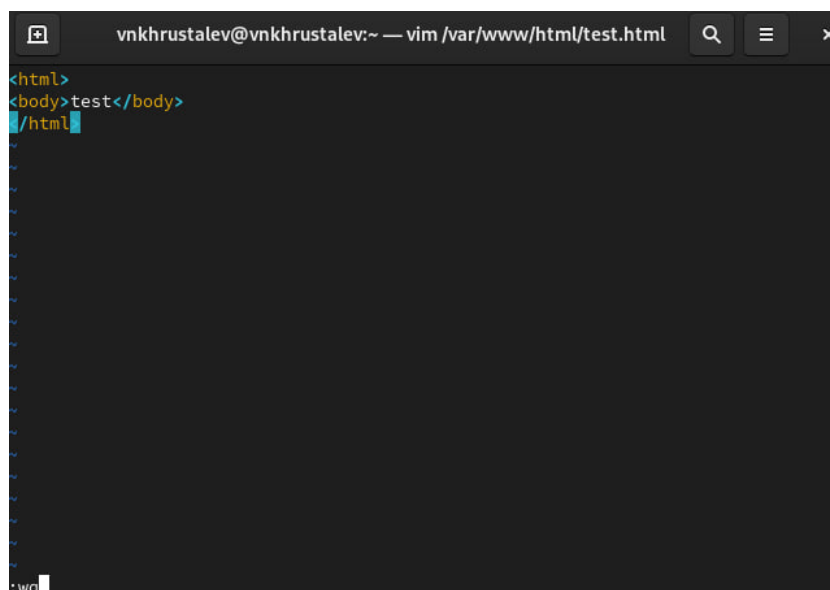


Рис. 2.7: Тип файлов и поддиректорий, находящихся в директории /var/www/html

4. Создание html файла, проверка его контекста и визуальный просмотр (рис. 2.8 и 2.9 и 2.10)

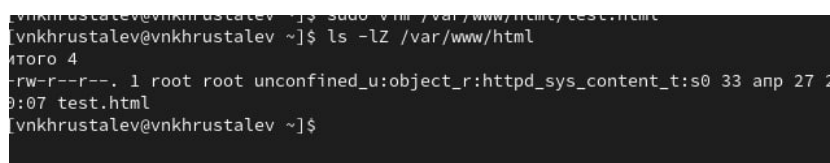


Рис. 2.8: Создание html-файл /var/www/html/test.html

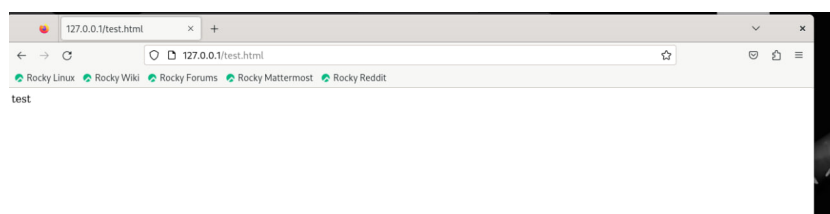


Рис. 2.9: Контекст созданного файла


```
[vnkhurstalev@vnkhurstalev ~]$ man httpd_selinux
Нет справочной страницы для httpd_selinux
[vnkhurstalev@vnkhurstalev ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[vnkhurstalev@vnkhurstalev ~]$
```

Рис. 2.10: Отображение на сайте

5. Просмотр инфо о команде `httpd_selinux` – она отсутствует (рис. 2.11)

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

Рис. 2.11: `man httpd_selinux`

6. Изменение контекста html файла на любой другой и попытка просмотра.
У нас нет доступа. Так же проверим логи. (рис. 2.12 и 2.13 и 2.14)

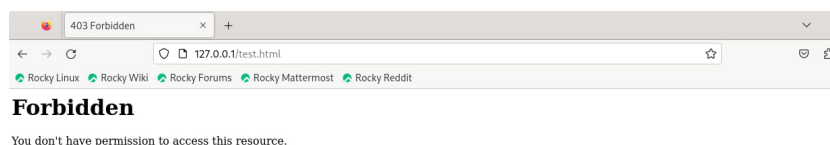


Рис. 2.12: Измените контекст файла `/var/www/html/test.html`


```
[root@vnxhrustalev vnxhrustalev]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module
               ,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
[root@vnxhrustalev vnxhrustalev]# 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@vnxhrustalev vnxhrustalev]#
```

Рис. 2.16: Перезапуск Apache

```
pegasus_http_port_t      tcp      5988
[root@vnxhrustalev vnxhrustalev]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vnxhrustalev vnxhrustalev]#
```

Рис. 2.17: Добавление порта 81 в разрешённые

8. Вернём всё обратно. Проверим что всё отображается. И попытаемся отключить порт 81, но не выйдет так как он уже используется и прописан в другом месте (рис. 2.19 и 2.18 и 2.20 и 2.21)

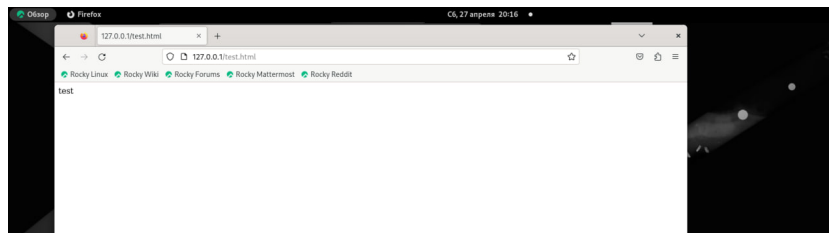


Рис. 2.18: Возврат стандарт контекста

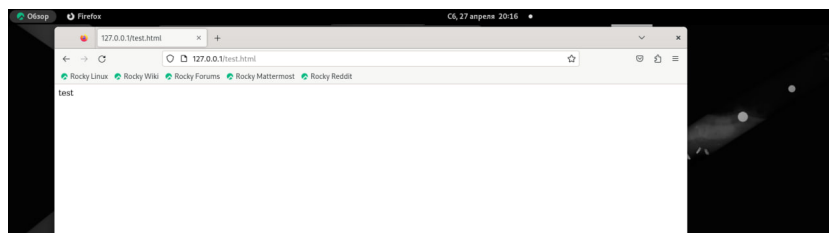


Рис. 2.19: Проверка сайта

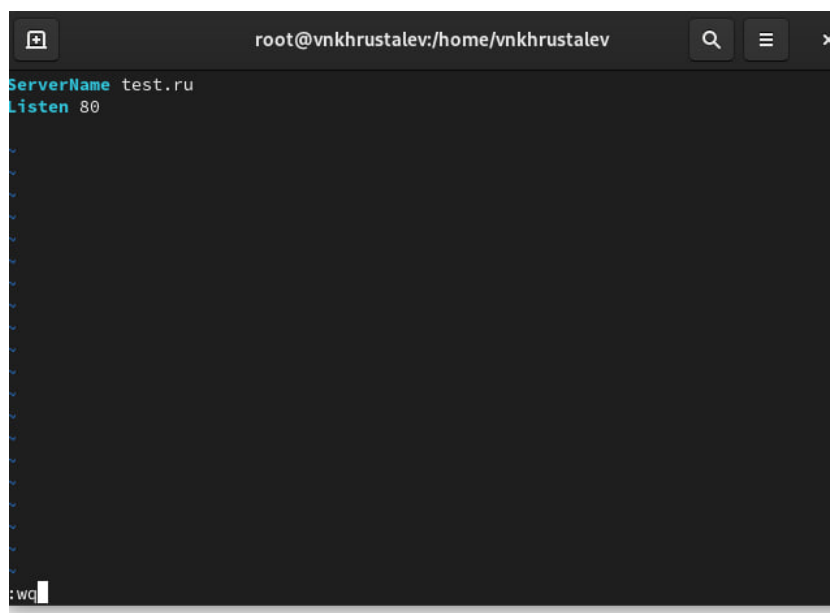


Рис. 2.20: Возврат стандартного порта

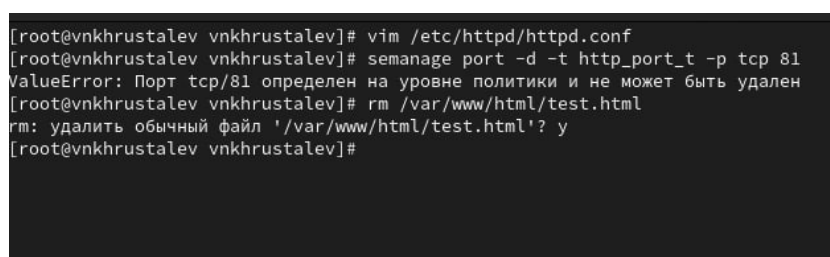


Рис. 2.21: Попытка отключения порта 81

3 Выводы

На данной лабораторной работе мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux.