

Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

1	Цель работы	5
2	Подготовка к лабораторной работе	6
3	Выполнение лабораторной работы	8
4	Вывод	19
	Список литературы	20

Список иллюстраций

2.1	Скачивание обновлений	6
2.2	Установка обновлений	6
2.3	Apache	7
3.1	SELinux режим	8
3.2	service httpd status	9
3.3	ps auxZ grep httpd	9
3.4	sestatus -bigrep httpd	10
3.5	seinfo	11
3.6	seinfo	11
3.7	seinfo	11
3.8	Создание файла test.html	12
3.9	Файл test.html	12
3.10	/var/www/html	12
3.11	Веб-сервер test.html	13
3.12	man httpd_selinux	13
3.13	man httpd_selinux	14
3.14	Ошибка	14
3.15	tail /var/log/messages	15
3.16	Listen 81	15
3.17	Сбой порта 81	16
3.18	/var/log/messages	16
3.19	/var/log/http/error_log	17
3.20	Порт 81	17
3.21	httpd_sys_content_t	18
3.22	httpd_sys_content_t	18
3.23	httpd_sys_content_t	18

Список таблиц

1 Цель работы

1. Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.
2. Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Подготовка к лабораторной работе

2.0.0.1 Скачиваем Apache

```
[adparathenko@adparathenko ~]$ sudo yum update
Rocky Linux 9 - BaseOS                               659 B/s | 4.1 kB      00:06
Rocky Linux 9 - BaseOS                               1.0 MB/s | 2.3 MB      00:02
Rocky Linux 9 - AppStream                             4.5 kB/s | 4.5 kB      00:01
Rocky Linux 9 - AppStream                             928 kB/s | 8.0 MB      00:08
Rocky Linux 9 - Extras                               5.0 kB/s | 2.9 kB      00:00
Dependencies resolved.
=====
Package Architecture Version Repository Size
=====
Installing:
kernel x86_64 5.14.0-427.37.1.el9_4 baseos 4.7 M
Upgrading:
NetworkManager x86_64 1:1.46.0-19.el9_4 baseos 2.3 M
NetworkManager-adsl x86_64 1:1.46.0-19.el9_4 baseos 35 k
NetworkManager-bluetooth x86_64 1:1.46.0-19.el9_4 baseos 61 k
NetworkManager-config-server noarch 1:1.46.0-19.el9_4 baseos 20 k
NetworkManager-libnm x86_64 1:1.46.0-19.el9_4 baseos 1.8 M
NetworkManager-team x86_64 1:1.46.0-19.el9_4 baseos 40 k
NetworkManager-tui x86_64 1:1.46.0-19.el9_4 baseos 245 k
NetworkManager-wifi x86_64 1:1.46.0-19.el9_4 baseos 83 k
NetworkManager-wwan x86_64 1:1.46.0-19.el9_4 baseos 68 k
bind-libs x86_64 32:9.16.23-18.el9_4.6 appstream 1.2 M
bind-license noarch 32:9.16.23-18.el9_4.6 appstream 13 k
bind-utils x86_64 32:9.16.23-18.el9_4.6 appstream 201 k
bpftool x86_64 7.3.0-427.37.1.el9_4 baseos 5.4 M
bubblewrap x86_64 0.4.1-7.el9_4 baseos 49 k
buildah x86_64 2:1.33.7-4.el9_4 appstream 9.4 M
c-ares x86_64 1.19.1-2.el9_4 baseos 110 k
ca-certificates noarch 2024.2.69_v8.0.303-91.4.el9_4 baseos 911 k
cockpit x86_64 311.2-1.el9_4 baseos 40 k
cockpit-bridge x86_64 311.2-1.el9_4 baseos 500 k
cockpit-packagekit noarch 311.2-1.el9_4 appstream 923 k
cockpit-storaged noarch 311.2-1.el9_4 appstream 853 k
cockpit-system noarch 311.2-1.el9_4 baseos 5.1 M
cockpit-ws x86_64 311.2-1.el9_4 baseos 915 k
containernetworking-plugins x86_64 1:1.4.0-5.el9_4 appstream 9.3 M
cups x86_64 1:2.3.30p2-27.el9_4 appstream 1.3 M
cups-client x86_64 1:2.3.30p2-27.el9_4 appstream 68 k
cups-filesystem noarch 1:2.3.30p2-27.el9_4 appstream 9.6 k
```

Рис. 2.1: Скачивание обновлений

```
systemd-udev-252-32.el9_4.7.x86_64
tar-2:1.34-6.el9_4.1.x86_64
wget-1.21.1-8.el9_4.x86_64
xfsdump-3.1.12-4.el9_3.x86_64
Installed:
composefs-1.0.3-2.el9.x86_64 composefs-libs-1.0.3-2.el9.x86_64
grub2-tools-efi-1:2.06-82.el9_4.x86_64 grub2-tools-extra-1:2.06-82.el9_4.x86_64
kernel-5.14.0-427.37.1.el9_4.x86_64 kernel-core-5.14.0-427.37.1.el9_4.x86_64
kernel-devel-5.14.0-427.37.1.el9_4.x86_64 kernel-modules-5.14.0-427.37.1.el9_4.x86_64
kernel-modules-core-5.14.0-427.37.1.el9_4.x86_64
Complete!
```

Рис. 2.2: Установка обновлений

```
[adparathenko@adparathenko ~]$ sudo yum -y install httpd
[sudo] password for adparathenko:
Last metadata expiration check: 0:38:46 ago on Mon 07 Oct 2024 11:05:28 PM MSK.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
httpd                  x86_64            2.4.57-11.el9_4.1  appstream         44 k
Installing dependencies:
apr                    x86_64            1.7.0-12.el9_3    appstream        122 k
apr-util               x86_64            1.6.1-23.el9      appstream         94 k
apr-util-bdb           x86_64            1.6.1-23.el9      appstream         12 k
httpd-core              x86_64            2.4.57-11.el9_4.1  appstream        1.4 M
httpd-filesystem        noarch            2.4.57-11.el9_4.1  appstream         11 k
httpd-tools             x86_64            2.4.57-11.el9_4.1  appstream         79 k
rocky-logos-httpd      noarch            90.15-2.el9       appstream         24 k
Installing weak dependencies:
apr-util-openssl        x86_64            1.6.1-23.el9      appstream         14 k
mod_http2               x86_64            2.0.26-2.el9_4    appstream        162 k
mod_lua                 x86_64            2.4.57-11.el9_4.1  appstream         58 k
=====
Transaction Summary
=====
Install 11 Packages

Total download size: 2.0 M
Installed size: 6.0 M
Downloading Packages:
(1/11): rocky-logos-httpd-90.15-2.el9.noarch.rpm                28 kB/s | 24 kB  00:00
(2/11): mod_lua-2.4.57-11.el9_4.1.x86_64.rpm                   50 kB/s | 58 kB  00:01
(3/11): httpd-tools-2.4.57-11.el9_4.1.x86_64.rpm                66 kB/s | 79 kB  00:01
(4/11): httpd-filesystem-2.4.57-11.el9_4.1.noarch.rpm           206 kB/s | 11 kB  00:00
(5/11): httpd-2.4.57-11.el9_4.1.x86_64.rpm                      105 kB/s | 44 kB  00:00
(6/11): apr-util-openssl-1.6.1-23.el9.x86_64.rpm               82 kB/s | 14 kB  00:00
(7/11): apr-util-bdb-1.6.1-23.el9.x86_64.rpm                   71 kB/s | 12 kB  00:00
(8/11): apr-util-1.6.1-23.el9.x86_64.rpm                       758 kB/s | 94 kB  00:00
```

Рис. 2.3: Apache

3 Выполнение лабораторной работы

- 1) Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме *enforcing* политики *targeted* с помощью команд *getenforce* и *sestatus*. (рис. 3.1)

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

Рис. 3.1: SELinux режим

- 2) Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: *service httpd status* (рис. 3.2)


```
[adparathenko@adparathenko ~]$ sudo systemctl start httpd
[sudo] password for adparathenko:
[adparathenko@adparathenko ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[adparathenko@adparathenko ~]$ 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 Mon 2024-10-07 23:51:53 MSK; 34s ago
     Docs: man:htpd.service(8)
    Main PID: 81022 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
      Tasks: 177 (limit: 12207)
     Memory: 26.3M
        CPU: 216ms
    CGroup: /system.slice/httpd.service
            └─81022 /usr/sbin/httpd -DFOREGROUND
              └─81023 /usr/sbin/httpd -DFOREGROUND
                └─81024 /usr/sbin/httpd -DFOREGROUND
                  └─81025 /usr/sbin/httpd -DFOREGROUND
                    └─81029 /usr/sbin/httpd -DFOREGROUND

Oct 07 23:51:52 adparathenko systemd[1]: Starting The Apache HTTP Server...
Oct 07 23:51:53 adparathenko httpd[81022]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, setting 'ServerName' to localhost.
Oct 07 23:51:53 adparathenko systemd[1]: Started The Apache HTTP Server.
Oct 07 23:51:53 adparathenko httpd[81022]: Server configured, listening on: port 80
lines 1-20/20 (END)
```

Рис. 3.2: service httpd status

- 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*** (рис. 3.3)

```
[adparathenko@adparathenko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      81022  0.0  0.5 20364 11336 ?        Ss   23:51   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  81023  0.0  0.3 22096  7248 ?        S    23:51   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  81024  0.0  0.5 981520 11064 ?       Sl   23:51   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  81025  0.0  0.8 1112656 17604 ?       Sl   23:51   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  81029  0.0  0.5 981520 11064 ?       Sl   23:51   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 adparat+ 81270 0.0  0.1 221796 2304 pts/0 S+   23:57   0:00 grep --color=auto httpd
```

Рис. 3.3: ps auxZ | grep httpd

- 4) Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды ***sestatus -bigrep httpd*** (рис. 3.4)

```
[adparathenko@adparathenko ~]$ 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
boinc_execmem                   on
cdrecord_read_content           off
cluster_can_network_connect     off
cluster_manage_all_files        off
cluster_use_execmem             off
cobbler_anon_write              off
cobbler_can_network_connect     off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect    off
colord_use_nfs                  off
condor_tcp_network_connect      off
```

Рис. 3.4: sestatus -bigrep httpd

- 5) Посмотрите статистику по политике с помощью команды **seinfo**, также определите множество пользователей, ролей, типов. (рис. 3.5)

```
[adparathenko@adparathenko ~]$ 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
[adparathenko@adparathenko ~]$
```

Рис. 3.5: seinfo

- 6) Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` (рис. 3.6)

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

Рис. 3.6: seinfo

- 7) Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Директория пуста. (рис. 3.7)

```
[adparathenko@adparathenko ~]$ ls -lZ /var/www/html
total 0
[adparathenko@adparathenko ~]$
```

Рис. 3.7: seinfo

- 8) Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` (рис. 3.8) - (рис. 3.9)

```
[adparathenko@adparathenko ~]$ sudo touch /var/www/html/test.html
[sudo] password for adparathenko:
[adparathenko@adparathenko ~]$ sudo gedit /var/www/html/test.html
```

Рис. 3.8: Создание файла test.html



Рис. 3.9: Файл test.html

- 9) Проверьте контекст созданного вами файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html` это ***httpd_sys_content*** (рис. 3.10)

```
[adparathenko@adparathenko ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[adparathenko@adparathenko ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct  8 00:08 test.html
[adparathenko@adparathenko ~]$
```

Рис. 3.10: `/var/www/html`

- 10) Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Файл был успешно отображён. (рис. 3.11)

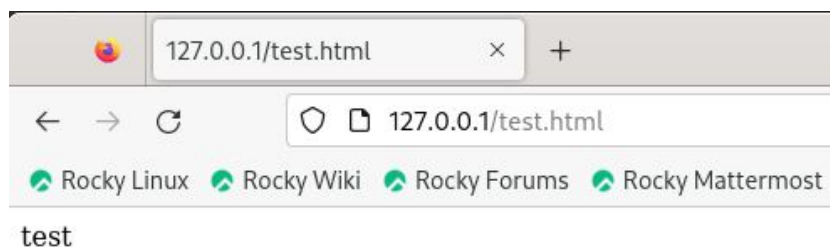


Рис. 3.11: Веб-сервер test.html

11) Изучите справку *man httpd_selinux*. (рис. 3.12)

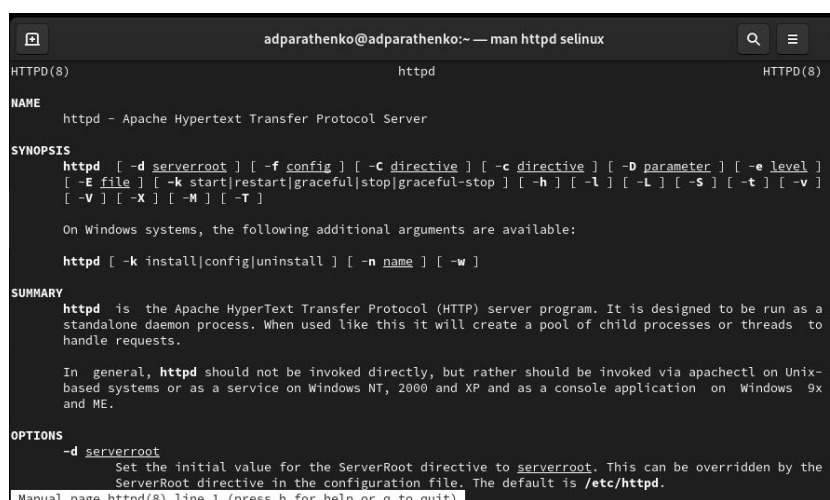


Рис. 3.12: man httpd_selinux

12) Проверить контекст файла можно командой ***ls -Z. ls -Z /var/www/html/test.html***

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*** (рис. 3.13)

```
[adparathenko@adparathenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[adparathenko@adparathenko ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_
ion not permitted
[adparathenko@adparathenko ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for adparathenko:
[adparathenko@adparathenko ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[adparathenko@adparathenko ~]$
```

Рис. 3.13: man httpd_selinux

- 13) Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес *http://127.0.0.1/test.html*. Получили сообщение об ошибке. (рис. 3.14)

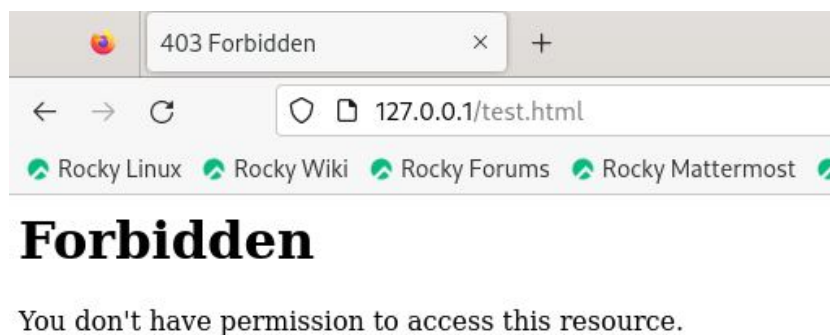


Рис. 3.14: Ошибка

- 14) Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: *tail /var/log/messages* (рис. 3.15)

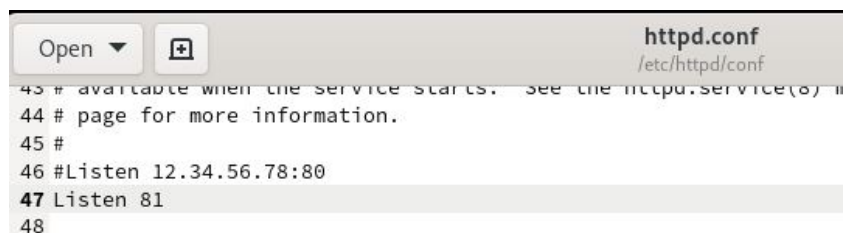
```

[adparathenko@adparathenko ~]$ ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 Oct  8 00:08 /var/www/html/test.html
[adparathenko@adparathenko ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[adparathenko@adparathenko ~]$ sudo tail /var/log/messages
Oct  8 00:16:52 adparathenko systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.Setroubleshoo
rileged.
Oct  8 00:16:52 adparathenko systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@.servic
Oct  8 00:16:58 adparathenko setroubleshoot[81900]: SELinux is preventing /usr/sbin/httpd from getattr access
the file /var/www/html/test.html. For complete SELinux messages run: sealert -l f719bd48-3613-46b9-81fb-9047b
6dc1f
Oct  8 00:16:58 adparathenko setroubleshoot[81900]: SELinux is preventing /usr/sbin/httpd from getattr access
the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****
*****#012#012If you want to fix the label, #012/var/www/html/test.html default label should be httpd_sys_co
ent_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permission
to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/r
storecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****
*****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.
ml to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/h
l/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) sugg
ts *****#012#012If you believe that httpd should be allowed getattr access on the test.
ml file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allo
this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M
-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct  8 00:16:58 adparathenko setroubleshoot[81900]: SELinux is preventing /usr/sbin/httpd from getattr access
the file /var/www/html/test.html. For complete SELinux messages run: sealert -l f719bd48-3613-46b9-81fb-9047b
6dc1f
Oct  8 00:16:58 adparathenko setroubleshoot[81900]: SELinux is preventing /usr/sbin/httpd from getattr access
the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****
*****#012#012If you want to fix the label, #012/var/www/html/test.html default label should be httpd_sys_co
ent_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permission
to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/r
storecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****
*****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.
ml to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/h
l/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) sugg
ts *****#012#012If you believe that httpd should be allowed getattr access on the test.
ml file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allo

```

Рис. 3.15: tail /var/log/messages

- 15) 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*. (рис. 3.16)



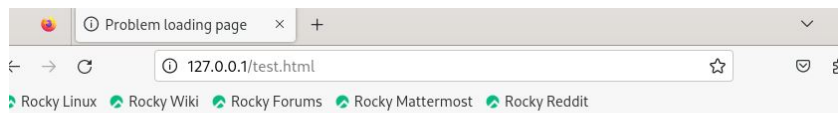
```

43 # available when the service starts.  See the httpd.service(8) m
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48

```

Рис. 3.16: Listen 81

- 16) Выполните перезапуск веб-сервера Apache. Произошел сбой. (рис. 3.17)



Unable to connect

Firefox can't establish a connection to the server at 127.0.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Рис. 3.17: Сбой порта 81

17) Проанализируйте лог-файлы: ***tail -nl /var/log/messages***. (рис. 3.18)

```
tail: cannot open '/var/log/messages' for reading: Permission denied
[adparathenko@adparathenko ~]$ sudo tail -nl /var/log/messages
Oct  8 00:28:19 adparathenko systemd[1]: setroubleshootd.service: Consumed 1.583s CPU time.
[adparathenko@adparathenko ~]$
```

Рис. 3.18: /var/log/messages

18) Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`. (рис. 3.19)


```

[adparathenko@adparathenko ~]$ sudo cat /var/log/httpd/error_log
[Mon Oct 07 23:51:53.149717 2024] [core:notice] [pid 81022:tid 81022] SELinux policy enabled; httpd running as c
ontext system_u:system_r:httpd_t:s0
[Mon Oct 07 23:51:53.159389 2024] [suexec:notice] [pid 81022:tid 81022] AH01232: suEXEC mechanism enabled (wrappe
er: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:fe9a
:1fdd%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Mon Oct 07 23:51:53.207315 2024] [lbmethod_heartbeat:notice] [pid 81022:tid 81022] AH02282: No slotmem from mod
_heartbeat
[Mon Oct 07 23:51:53.243089 2024] [mpm_event:notice] [pid 81022:tid 81022] AH00489: Apache/2.4.57 (Rocky Linux)
configured -- resuming normal operations
[Mon Oct 07 23:51:53.243153 2024] [core:notice] [pid 81022:tid 81022] AH00094: Command line: '/usr/sbin/httpd -D
FOREGROUND'
[Tue Oct 08 00:16:46.687054 2024] [core:error] [pid 81029:tid 81186] (13)Permission denied: [client 127.0.0.1:51
880] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:22:55.838355 2024] [core:error] [pid 81029:tid 81188] (13)Permission denied: [client 127.0.0.1:49
518] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:22:58.939589 2024] [core:error] [pid 81029:tid 81189] (13)Permission denied: [client 127.0.0.1:49
518] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:23:10.967707 2024] [core:error] [pid 81029:tid 81192] (13)Permission denied: [client 127.0.0.1:58
382] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:24:36.780030 2024] [core:error] [pid 81029:tid 81196] (13)Permission denied: [client 127.0.0.1:53
810] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:24:39.260800 2024] [core:error] [pid 81029:tid 81197] (13)Permission denied: [client 127.0.0.1:53
810] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:24:39.990010 2024] [core:error] [pid 81029:tid 81198] (13)Permission denied: [client 127.0.0.1:53
810] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:25:39.883445 2024] [core:error] [pid 81029:tid 81202] (13)Permission denied: [client 127.0.0.1:43
514] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Tue Oct 08 00:26:48.709524 2024] [core:error] [pid 81029:tid 81194] (13)Permission denied: [client 127.0.0.1:33
948] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path

```

Рис. 3.19: /var/log/httpd/error_log

- 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***. Порт 81 появился в списке. (рис. 3.20)

```

[adparathenko@adparathenko ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[adparathenko@adparathenko ~]$ semanage port -l | grep http_port_t
semanage port: error: one of the arguments -a/--add -d/--delete -m/--modify -l/--list -E/--extract -D/--del
l is required
[adparathenko@adparathenko ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[adparathenko@adparathenko ~]$ 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
[adparathenko@adparathenko ~]$

```

Рис. 3.20: Порт 81

- 20) Попробуйте запустить веб-сервер Apache ещё раз. Сейчас запустился. 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***. Видим содержимое файла. (рис. 3.21)

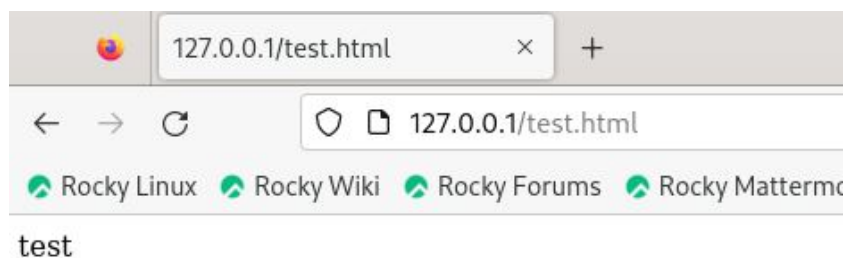


Рис. 3.21: httpd_sys_content_t

- 21) Исправьте обратно конфигурационный файл apache, вернув Listen 80. Удалите привязку `http_port_t` к 81 порту: ***semanage port -d -t http_port_t -p tcp 81*** и проверьте, что порт 81 удалён. (рис. 3.22)

```
[adparathenko@adparathenko ~]$ 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
[adparathenko@adparathenko ~]$ sudo semanage port -d -t http_port_t -p tcp 81
[adparathenko@adparathenko ~]$ sudo 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
```

Рис. 3.22: httpd_sys_content_t

- 22) Удалите файл `/var/www/html/test.html`: ***rm /var/www/html/test.html*** (рис. 3.23)

```
[adparathenko@adparathenko ~]$ sudo rm /var/www/html/test.html
[adparathenko@adparathenko ~]$ ls -lZ /var/www/html
total 0
[adparathenko@adparathenko ~]$
```

Рис. 3.23: httpd_sys_content_t

4 Вывод

В результате выполнения работы мы получили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux¹, а также проверили работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

- 1) https://esystem.rudn.ru/pluginfile.php/2357155/mod_resource/content/2/006-lab_selinux.pdf