

Nº 6

Linux

, ,

SELinx

Linux.

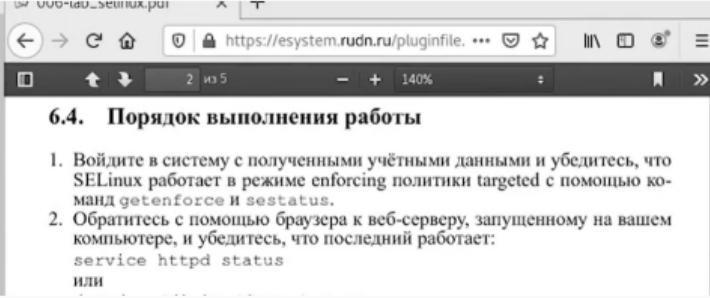
-

Apache.

SELinux1.

targeted , SELinux enforcing
getenforce sestatus.

```
[root@kazabolo ~]# getenforce
Enforcing
[root@kazabolo ~]# 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
Max kernel policy version: 31
[root@kazabolo ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
```



. 1: getenforce, sestatus

: service

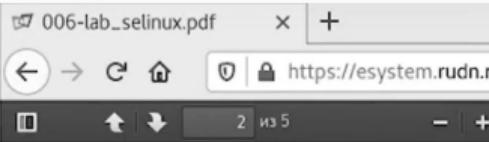
httpd status

```

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
Max kernel policy version:    31
[root@kazabolo html]# 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; vendor
   preset: disabled)
     Active: active (running) since Пт 2021-11-26 16:57:24 MSK; 1min 57s ago
       Docs: man:httpd(8)
              man:apachectl(8)
   Main PID: 7114 (httpd)
     Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
 0 B/sec"
      Tasks: 6
     CGroup: /system.slice/httpd.service
             ├─7114 /usr/sbin/httpd -DFOREGROUND
             ├─7119 /usr/sbin/httpd -DFOREGROUND
             ├─7120 /usr/sbin/httpd -DFOREGROUND
             ├─7121 /usr/sbin/httpd -DFOREGROUND
             ├─7122 /usr/sbin/httpd -DFOREGROUND
             ├─7123 /usr/sbin/httpd -DFOREGROUND

ноя 26 16:57:24 zikarimov.localdomain systemd[1]: Starting The Apache...
ноя 26 16:57:24 zikarimov.localdomain systemd[1]: Started The Apache...
Hint: Some lines were ellipsized, use -l to show in full.

```



6.4. Порядок выполнения работы

1. Войдите в систему с полученными учётными данными. SELinux работает в режиме enforcing мандатов `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к вашему компьютеру, и убедитесь, что последний запущен. Выполните команду `service httpd status` или `/etc/rc.d/init.d/httpd status`. Если не работает, запустите его так же.
3. Найдите веб-сервер Apache в списке параметров безопасности и занесите эту информацию в таблицу. Используйте команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`.
4. Посмотрите текущее состояние перезапуска веб-сервера с помощью команды `sestatus -bigrep httpd`. Обратите внимание, что многие из них не работают.

Активные
Чтобы

. 2: service httpd status

- Apache

```
ps auxZ | grep httpd
```

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      7114  0.0  0.2 224084  5016 ?
Ss 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    7119  0.0  0.1 226168  3092 ?
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    7120  0.0  0.1 226168  3092 ?
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    7121  0.0  0.1 226168  3092 ?
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    7122  0.0  0.1 226168  3092 ?
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    7123  0.0  0.1 226168  3092 ?
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 7273 0.0  0.0 1
12832 976 pts/0 S+ 16:59 0:00 grep --color=auto httpd
[root@kazabolo ~]# sestatus -b | grep httpd
```

006-lab_selinux.pdf
https://esystem.rudn.ru/
2 из 5

/etc/rc.d/init.d/httpd status
Если не работает, запустите его так же.

3. Найдите веб-сервер Apache в списке пр
безопасности и занесите эту информац
пользовать команду
ps auxZ | grep httpd
или
ps -eZ | grep httpd

4. Посмотрите текущее состояние перек
помощью команды
sestatus -b
Обратите внимание, что многие из них

. 3: ps auxZ | grep httpd

SELinux Apache
«off».

`sestatus -bigrep httpd`

```
S 16:57 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 7273 0.0 0.0 1
12832 976 pts/0 S+ 16:59 0:00 grep --color=auto httpd
[root@zikarimov ~]# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown on
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
```

006-lab_selinux.pdf x +

← → C ⌂ 2 из 5 - +

/etc/rc.d/init.d/httpd status
Если не работает, запустите его так же

- Найдите веб-сервер Apache в списке правил безопасности и занесите эту информацию в таблицу
- Посмотрите текущее состояние правил безопасности с помощью команды
ps auxZ | grep httpd
или
ps -eZ | grep httpd
- Обратите внимание, что многие из них

42 Кулажин Активность

5. Посмотрите статистику по политике с правами root. Определите множество пользователей.

. 4: ps auxZ | grep httpd

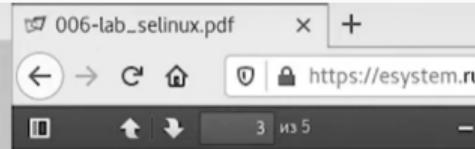
seinfo,

, , .

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130    Permissions:      272
Sensitivities:    1      Categories:     1024
Types:           4793    Attributes:      253
Users:            8      Roles:          14
Booleans:         316    Cond. Expr.:   362
Allow:          107834   Neverallow:     0
Auditallow:       158    Dontaudit:    10022
Type_trans:       18153   Type_change:   74
Type_member:      35     Role allow:   37
Role_trans:        414    Range_trans:  5899
Constraints:      143    Validatetrans: 0
Initial SIDs:     27     Fs_use:        32
Genfscon:         103    Portcon:      614
Netifcon:          0     Nodecon:      0
Permissives:      0     Polcap:        5
```

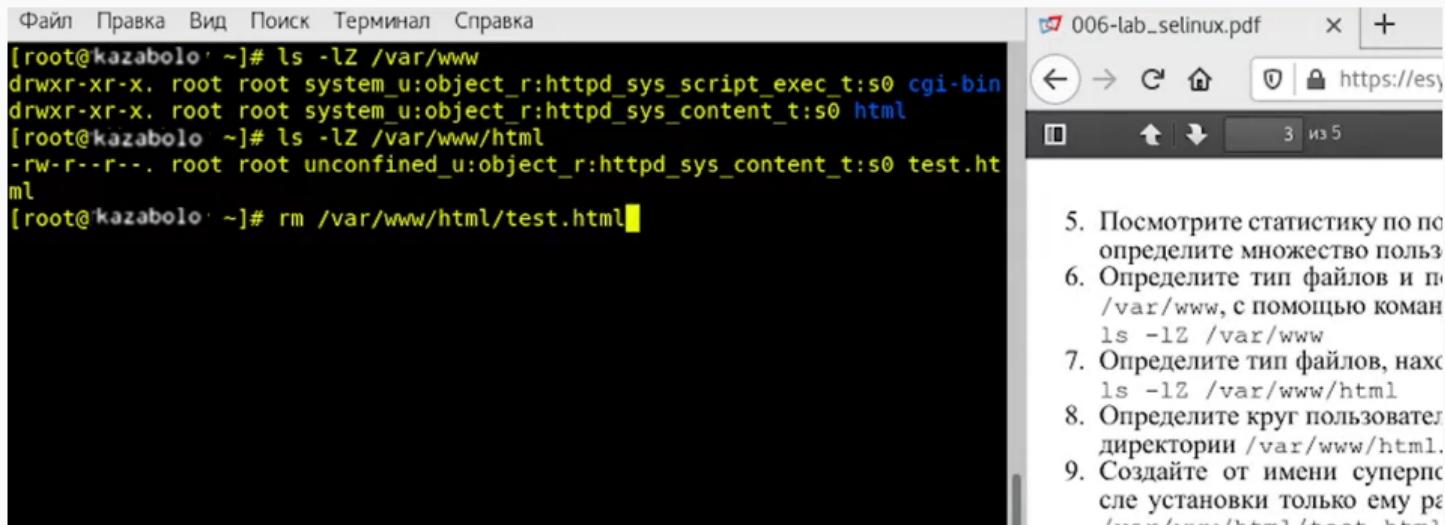


5. Посмотрите статистику по политики определите множество пользователей
6. Определите тип файлов и поддиректорий `/var/www`, с помощью команды `ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`.
8. Определите круг пользователей, к которым относится директория `/var/www/html`.
9. Создайте от имени суперпользователя установки только ему разрешения на файл `/var/www/html/test.html` следующим образом:
`<html>`
`<header>+a+a+</header>`

. 5: seinfo

/var/www, ls -lZ /var/www.
/var/www/html: ls -lZ /var/www/html.
 /var/www/html.

Файл Правка Вид Поиск Терминал Справка

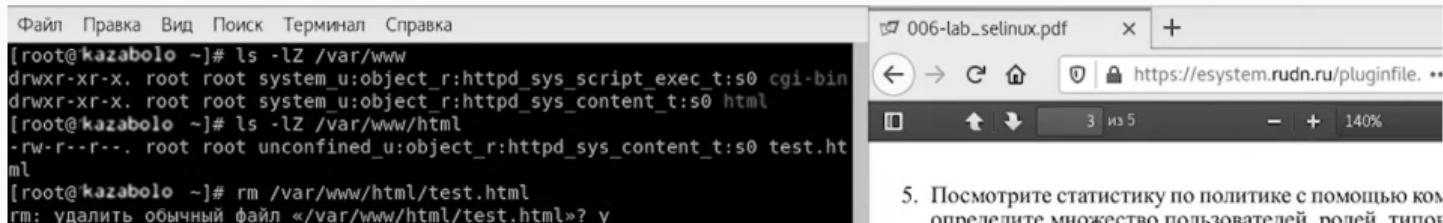


```
[root@kazabolo: ~]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@kazabolo ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@kazabolo ~]# rm /var/www/html/test.html
```

006-lab_selinux.pdf x +
← → G ⌂ https://esy
[] ↑ ↓ 3 из 5

5. Посмотрите статистику по по определите множество польз
6. Определите тип файлов и по /var/www, с помощью коман ls -lZ /var/www
7. Определите тип файлов, находящиеся в директории /var/www/html.
8. Определите круг пользователей, имеющих доступ к директории /var/www/html.
9. Создайте от имени суперпользователя файл test.html в директории /var/www/html. Установите для него права 644.

. 6: /var/www



Файл Правка Вид Поиск Терминал Справка

```
[root@kazabolo ~]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@kazabolo ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@kazabolo ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
```

006-lab_selinux.pdf x +
← → C ⌂ https://esystem.rudn.ru/pluginfile..
□ ↑ ↓ 3 из 5 - + 140%

5. Посмотрите статистику по политике с помощью команда определите множество пользователей полей типов

. 7: /var/www

Файл Правка Вид Поиск Терминал Справка

```
[root@kazabolo ~]# ls -lZ /var/www/html
[root@kazabolo ~]# touch /var/www/html/test.html
[root@kazabolo ~]# vim /var/www/html/test.html
```

006-lab_selinux.pdf x +

← → ⌂ ⌂ https://esystem.rudn.ru/pluginfil

□ ↕ 3 из 5 - + 140%

определите множество пользователей, ролей, ти
6. Определите тип файлов и поддиректорий, нах

. 8: /var/www

html- /var/www/html/test.html.

```
<html>
<body>
test
</body>
</html>
```

006-lab_selinux.pdf x +

https://esysten

3 из 5

определите множество пользователей

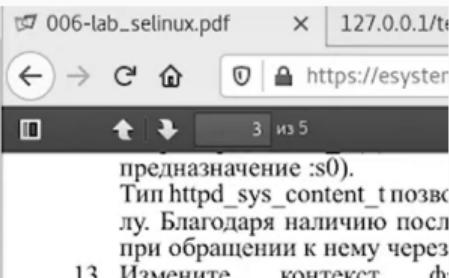
6. Определите тип файлов и поддиректорий в директории /var/www, с помощью команды ls -lZ /var/www
7. Определите тип файлов, находящихся в директории /var/www/html
8. Определите круг пользователей, имеющих доступ к директории /var/www/html.
9. Создайте от имени суперпользователя файл test.html в директории /var/www/html/test.html следующего содержания:

```
<html>
<body>test</body>
</html>
```
10. Проверьте контекст созданного файла test.html, присваиваемый по умолчанию в директории /var/www/html.
11. Обратитесь к файлу через веб-браузер по адресу http://127.0.0.1/test.html и убедитесь, что он отображён.
12. Изучите справку man httpd и определите, каким образом файлы определены для директории /var/www/html/test.html. Проверить контекст файлов в директории ls -Z /var/www/html/test.html

Рассмотрим полученный контекст

. 9: /var/www/html/test.html

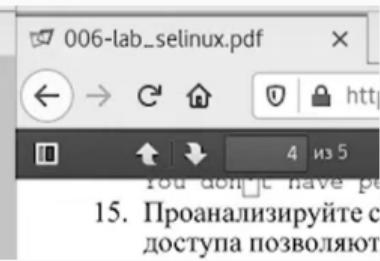
```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# ls -lZ /var/www/html
[root@kazabolo ~]# touch /var/www/html/test.html
[root@kazabolo ~]# vim /var/www/html/test.html
[root@kazabolo ~]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.htm
ml
[root@kazabolo ~]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```



. 10: /var/www/html

```
chon -t samba_share_t /var/www/html/test/html
```

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# chcon -t samba_share_t /var/www/html/test.html
[root@kazabolo ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 test.html
[root@kazabolo ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 37 ноя 26 17:02 /var/www/html/test.html
[root@kazabolo ~]# tail /var/log/messages
```



. 11: chon -t samba_share_t /var/www/html/test/html

```
/var/www/html/test.html httpd_sys_content_t ,  
httpd , , samba_share_t: chcon -t samba_share_t  
/var/www/html/test.html, ls -Z /var/www/html/test.html
```

Файл Правка Вид Поиск Терминал Справка

```
cuting:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semo
dule -i my-httpd.pp#012
Nov 26 17:05:39 zikarimov dbus[698]: [system] Activating service name='org
.fedoraproject.Setroubleshootd' (using servicehelper)
Nov 26 17:05:40 zikarimov dbus[698]: [system] Successfully activated servi
ce 'org.fedoraproject.Setroubleshootd'
Nov 26 17:05:40 zikarimov setroubleshoot: failed to retrieve rpm info for
/var/www/html/test.html
Nov 26 17:05:41 zikarimov setroubleshoot: SELinux is preventing httpd from
getattr access on the file /var/www/html/test.html. For complete SELinux
messages run: sealert -l f3bc0461-1a7c-45cd-b36a-bb5c877ae4ca
Nov 26 17:05:41 zikarimov python: SELinux is preventing httpd from getattr
access on the file /var/www/html/test.html.#012#012***** Plugin restorec
on (92.2 confidence) suggests *****#012#012If you wan
t to fix the label. #012/var/www/html/test.html default label should be ht
tpd_sys_content_t.#012Then you can run restorecon. The access attempt may
have been stopped due to insufficient permissions to access a parent direc
tory in which case try to change the following command accordingly.#012Do#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin publ
ic_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.html to public_content_t or public_content_rw_t.#012Do#012#
semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# re
storecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41
confidence) suggests *****#012#012If you believe th
at httpd should be allowed getattr access on the test.html file by default
.#012Then you should report this as a bug.#012You can generate a local pol
icy module to allow this access.#012Do#012allow this access for now by exe
cuting:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semo
dule -i my-httpd.pp#012
[root@zikarimov ~]#
```

006-lab_selinux.pdf

← → ⌂ ⌂ https://

4 из 5

You don't have permission to access this resource.

15. Проанализируйте системные логи, чтобы определить, каким способом пользователи получают доступ к сайту. Для этого выполните команду `ls -l /var/www/html`. Просмотрите `log`-файл и системный лог-файл: `tail /var/log/messages`. Если в системе ошибка `auditd`, то вы также сможете это увидеть выше, в файле `/var/log/audit/audit.log`. Выполните команду `tail -n 10 /var/log/audit/audit.log`. Если в системе ошибка `auditd`, то вы также сможете это увидеть выше, в файле `/var/log/audit/audit.log`. Выполните команду `tail -n 10 /var/log/audit/audit.log`.
16. Попробуйте запустить веб-сервер на порт 81 (а не 80, как рекомендуется по умолчанию) вместо этого в файле `/etc/httpd/conf.d/welcome.conf` замените её на `Listens 81`.
17. Выполните перезапуск веб-сервера и проверьте, почему?
18. Проанализируйте логи в файле `/var/log/audit/audit.log`. Просмотрите `tail -n 10 /var/log/audit/audit.log`. Выясните, в каких файлах веб-сервера веб-страницы хранятся.
19. Выполните команду `semanage port -a --name httpd --port 81`. После этого проверьте, что веб-сервер работает на порте 81.

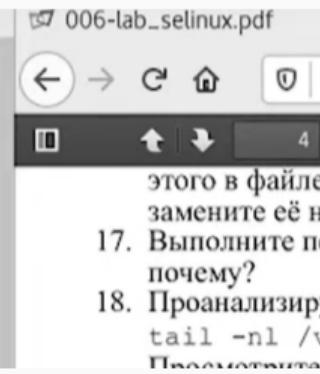
```
-l /var/www/html/test.html  
tail /var/log/messages.
```

```
,  
log- - Apache.  
setroubleshootd audtd,  
, /var/log/audit/audit.log
```

? ls

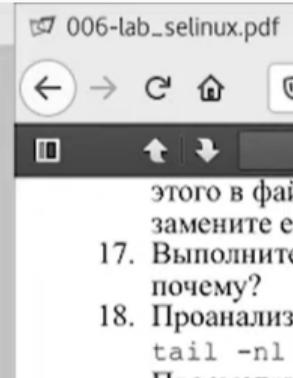
- :

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# restart httpd
bash: restart: команда не найдена...
[root@kazabolo ~]# systemctl httpd restart
Unknown operation 'httpd'.
[root@kazabolo ~]# systemctl restart httpd
[root@kazabolo ~]# tail -nl /var/log/messages
tail: l: неверное число строк
[root@kazabolo ~]# tail -n /var/log/messages
tail: /var/log/messages: неверное число строк
[root@kazabolo ~]# tail -nl /var/log/messages
tail: l: неверное число строк
```



. 13: tail /var/log/messages

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# restart httpd
bash: restart: команда не найдена...
[root@kazabolo ~]# systemctl httpd restart
Unknown operation 'httpd'.
[root@kazabolo ~]# systemctl restart httpd
[root@kazabolo ~]# tail -nl /var/log/messages
tail: l: неверное число строк
[root@kazabolo ~]# tail -n /var/log/messages
tail: /var/log/messages: неверное число строк
[root@kazabolo ~]# tail -nl /var/log/messages
tail: l: неверное число строк
```



. 14: tail /var/log/messages

Файл Правка Вид Поиск Терминал Справка

```
Nov 26 17:05:41 zikarimov python: SELinux is preventing httpd from getattr access on 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_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -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.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
```

Nov 26 17:07:58 zikarimov dbus[698]: [system] Activating service name='org.freedesktop.problems' (using servicehelper)

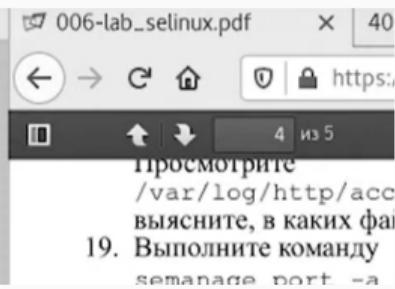
Nov 26 17:07:59 zikarimov dbus[698]: [system] Successfully activated service 'org.freedesktop.problems'

006-lab_selinux.pdf x 403 Forbidden
← → C ⌂ https://esystem.rudn.ru/pl...
□ ↑ ↓ 4 из 5 - + 14
этого в файле /etc/httpd/httpd.conf замените её на Listen 81.
17. Выполните перезапуск веб-сервера Apache почему?
18. Проанализируйте лог-файлы:
tail -nl /var/log/messages
Просмотрите файлы /var/log/http/access_log и /var/log/http/error_log, выясните, в каких файлах появились записи.
19. Выполните команду
semanage port -a -t http_port_t
После этого проверьте список портов в списке semanage port -l | grep http_port_t. Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache он сейчас запустился, а в предыдущем
21. Верните контекст httpd_sys_content_t
chcon -t httpd_sys_content_t /var/www/html/test.html

. 15: result

```
http_port_t 81      : semanage port -d -t http_port_t -p tcp 81      ,  
81      .      /var/www/html/test.html: rm /var/www/html/test.htm.
```

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kazabolo ~]# 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@kazabolo ~]# systemctl httpd restart
Unknown operation 'httpd'.
[root@kazabolo ~]# systemctl restart httpd
```



. 16: semanage port -d -t http_port_t -p tcp 81

```
Файл Правка Вид Поиск Терминал Справка
[root@kazabolo ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@kazabolo ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? у
[root@kazabolo ~]# ls -lZ /var/www/
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@kazabolo ~]# ls -lZ /var/www/html/
```



. 17: ls -lZ /var/www/html

SELinux1.

SELinx

Linux.

-
Apache.