Основы информационной безопасности. Лабораторная работа №6

Мандатное разграничение прав в Linux

Нзита Диатезилуа Катенди

12.10.2024

Российский Университет дружбы народов

Информация

Докладчик

- ДНзита Диатезилуа Катенди
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/NzitaKatendi

!

Вводная часть

Цели и задачи

Целью данной работы является приобретение практических навыков администрирования ОС Linux.

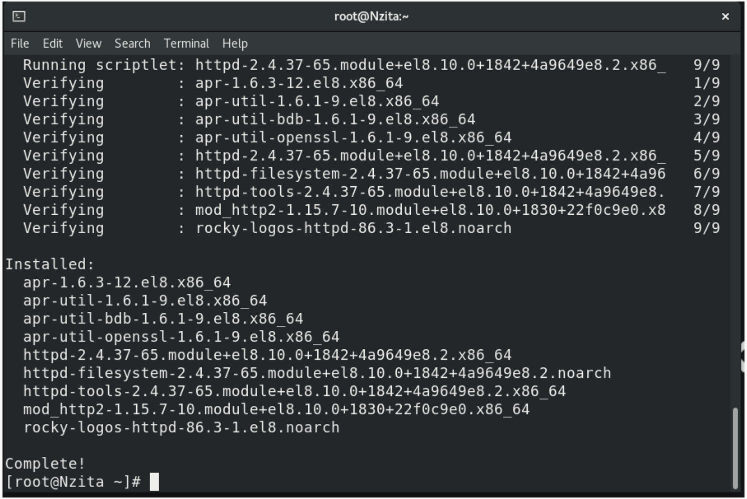
Задачи:

- Получить первое практическое знакомство с технологией SELinux.
- Проверить работу SELinx на практике совместно с веб-сервером Apache.

Инструмент: VirtualBox

Выполнение лабораторной работы

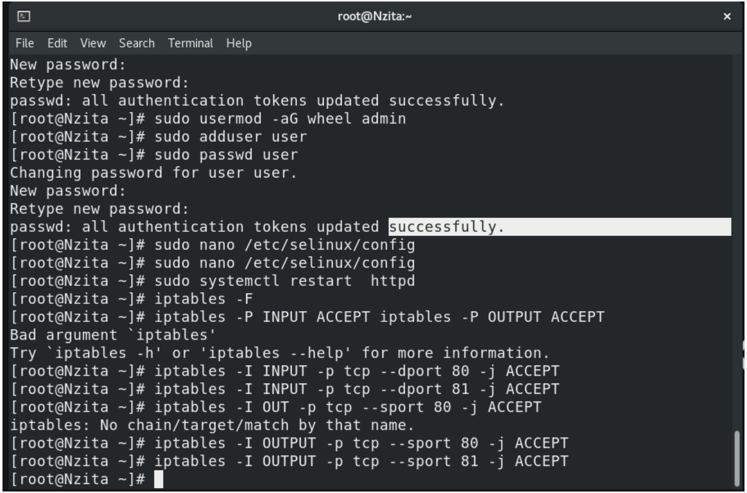
Подготовка лабораторного стенда



```
  Running scriptlet: httpd-2.4.37-65.module+el8.10.0+1842+4a9649e8.2.x86_   9/9
  Verifying        : apr-1.6.3-12.el8.x86_64                                1/9
  Verifying        : apr-util-1.6.1-9.el8.x86_64                            2/9
  Verifying        : apr-util-bdb-1.6.1-9.el8.x86_64                        3/9
  Verifying        : apr-util-openssl-1.6.1-9.el8.x86_64                    4/9
  Verifying        : httpd-2.4.37-65.module+el8.10.0+1842+4a9649e8.2.x86_   5/9
  Verifying        : httpd-filesystem-2.4.37-65.module+el8.10.0+1842+4a96   6/9
  Verifying        : httpd-tools-2.4.37-65.module+el8.10.0+1842+4a9649e8.   7/9
  Verifying        : mod_http2-1.15.7-10.module+el8.10.0+1830+22f0c9e0.x8   8/9
  Verifying        : rocky-logos-httpd-86.3-1.el8.noarch                    9/9

Installed:
  apr-1.6.3-12.el8.x86_64
  apr-util-1.6.1-9.el8.x86_64
  apr-util-bdb-1.6.1-9.el8.x86_64
  apr-util-openssl-1.6.1-9.el8.x86_64
  httpd-2.4.37-65.module+el8.10.0+1842+4a9649e8.2.x86_64
  httpd-filesystem-2.4.37-65.module+el8.10.0+1842+4a9649e8.2.noarch
  httpd-tools-2.4.37-65.module+el8.10.0+1842+4a9649e8.2.x86_64
  mod_http2-1.15.7-10.module+el8.10.0+1830+22f0c9e0.x86_64
  rocky-logos-httpd-86.3-1.el8.noarch

Complete!
[root@Nzita ~]# 
```

Рис. 1: Подготовка лабораторного стенда

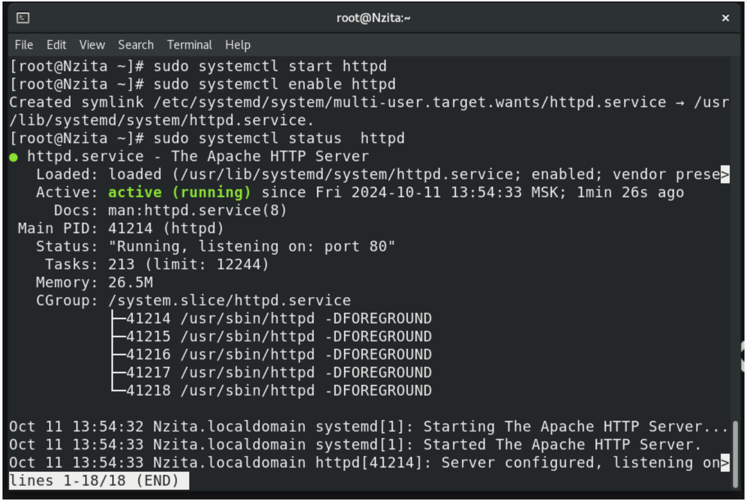
Практическое знакомтсво с технологией SELinux



```
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@Nzita ~]# sudo usermod -aG wheel admin
[root@Nzita ~]# sudo adduser user
[root@Nzita ~]# sudo passwd user
Changing password for user user.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@Nzita ~]# sudo nano /etc/selinux/config
[root@Nzita ~]# sudo nano /etc/selinux/config
[root@Nzita ~]# sudo systemctl restart  httpd
[root@Nzita ~]# iptables -F
[root@Nzita ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@Nzita ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@Nzita ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@Nzita ~]# iptables -I OUT -p tcp --sport 80 -j ACCEPT
iptables: No chain/target/match by that name.
[root@Nzita ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@Nzita ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@Nzita ~]#
```

Рис. 2: Проверка статуса SELinux

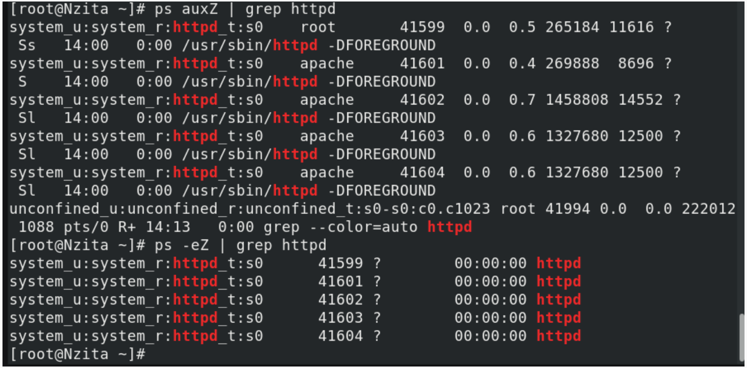
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# sudo systemctl start httpd
[root@Nzita ~]# sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
[root@Nzita ~]# sudo systemctl status  httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese>
   Active: active (running) since Fri 2024-10-11 13:54:33 MSK; 1min 26s ago
     Docs: man:httpd.service(8)
 Main PID: 41214 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 12244)
   Memory: 26.5M
   CGroup: /system.slice/httpd.service
           ├─41214 /usr/sbin/httpd -DFOREGROUND
           ├─41215 /usr/sbin/httpd -DFOREGROUND
           ├─41216 /usr/sbin/httpd -DFOREGROUND
           ├─41217 /usr/sbin/httpd -DFOREGROUND
           └─41218 /usr/sbin/httpd -DFOREGROUND

Oct 11 13:54:32 Nzita.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 11 13:54:33 Nzita.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 11 13:54:33 Nzita.localdomain httpd[41214]: Server configured, listening on>
lines 1-18/18 (END)
```

Рис. 3: Проверка статуса веб-сервера

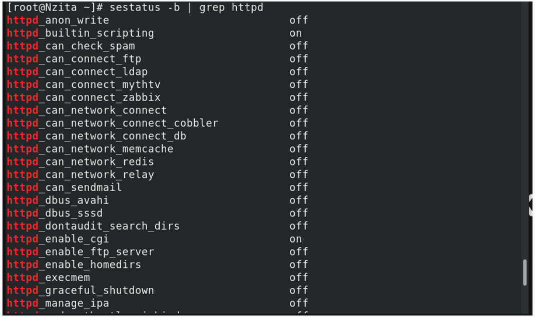
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       41599  0.0  0.5 265184 11616 ?
 Ss   14:00   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41601  0.0  0.4 269888  8696 ?
 S    14:00   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41602  0.0  0.7 1458808 14552 ?
 Sl   14:00   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41603  0.0  0.6 1327680 12500 ?
 Sl   14:00   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     41604  0.0  0.6 1327680 12500 ?
 Sl   14:00   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 41994 0.0  0.0 222012
 1088 pts/0 R+ 14:13   0:00 grep --color=auto httpd
[root@Nzita ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      41599 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      41601 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      41602 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      41603 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      41604 ?        00:00:00 httpd
[root@Nzita ~]#
```

Рис. 4: Просмотр контекста безопасности веб-сервера

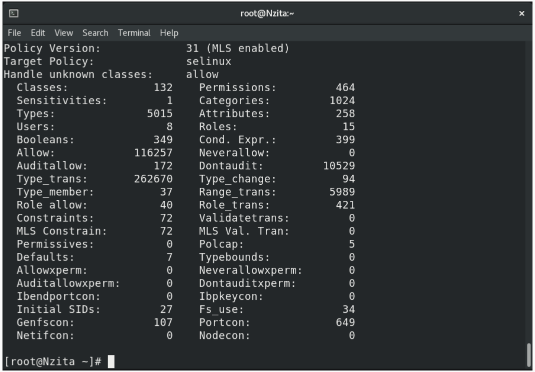
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# 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_redis                     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                     off
httpd_manage_ipa                            off
```

Рис. 5: Состояние переключателей SELinux для Apache

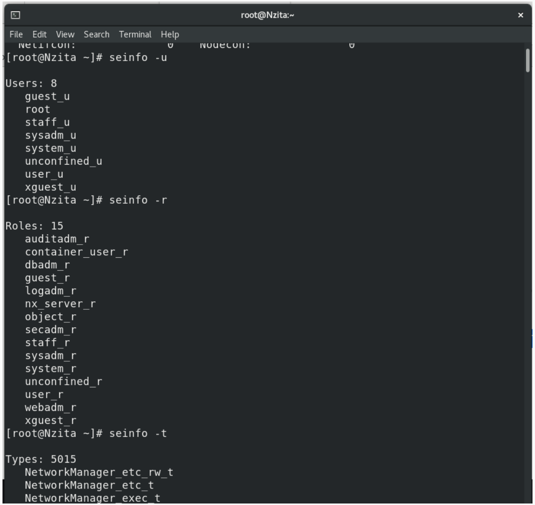
Практическое знакомтсво с технологией SELinux



```
Policy Version:             31 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             132    Permissions:         464
  Sensitivities:         1    Categories:         1024
  Types:              5015    Attributes:          258
  Users:                 8    Roles:                15
  Booleans:            349    Cond. Expr.:         399
  Allow:            116257    Neverallow:            0
  Auditallow:          172    Dontaudit:         10529
  Type_trans:       262670    Type_change:          94
  Type_member:          37    Range_trans:        5989
  Role allow:           40    Role_trans:          421
  Constraints:          72    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               34
  Genfscon:            107    Portcon:             649
  Netifcon:              0    Nodecon:               0

[root@Nzita ~]# 
```

Рис. 6: Статистика по политике

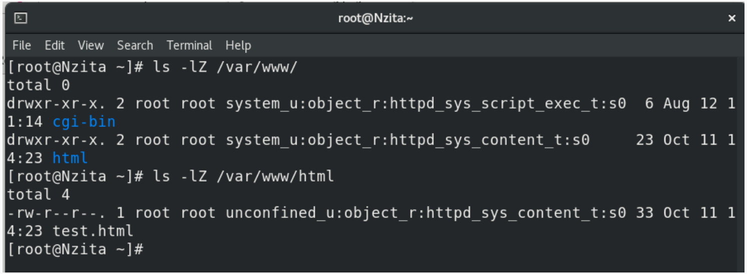
Практическое знакомтсво с технологией SELinux



```
  NetIfcon:             0    Nodecon:             0
[root@Nzita ~]# seinfo -u

Users: 8
   guest_u
   root
   staff_u
   sysadm_u
   system_u
   unconfined_u
   user_u
   xguest_u
[root@Nzita ~]# seinfo -r

Roles: 15
   auditadm_r
   container_user_r
   dbadm_r
   guest_r
   logadm_r
   nx_server_r
   object_r
   secadm_r
   staff_r
   sysadm_r
   system_r
   unconfined_r
   user_r
   webadm_r
   xguest_r
[root@Nzita ~]# seinfo -t

Types: 5015
   NetworkManager_etc_rw_t
   NetworkManager_etc_t
   NetworkManager_exec_t
```

Рис. 7: Множества пользователей, ролей, типов

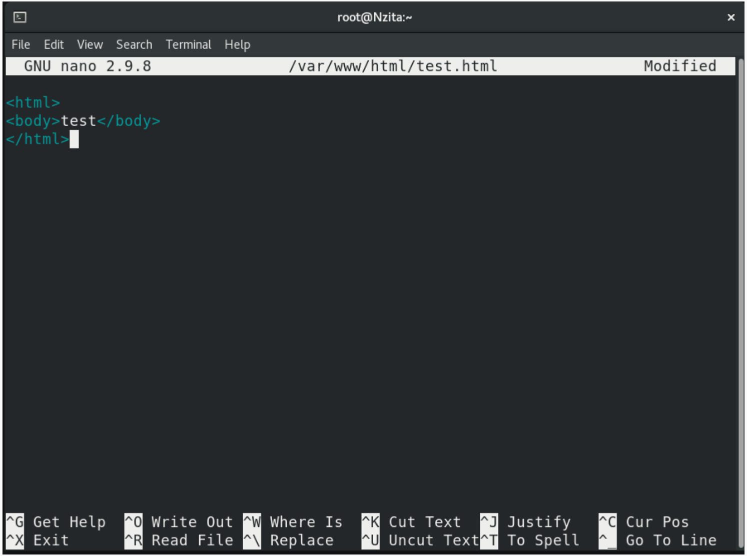
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0  6 Aug 12 1
1:14 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     23 Oct 11 1
4:23 html
[root@Nzita ~]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct 11 1
4:23 test.html
[root@Nzita ~]#
```

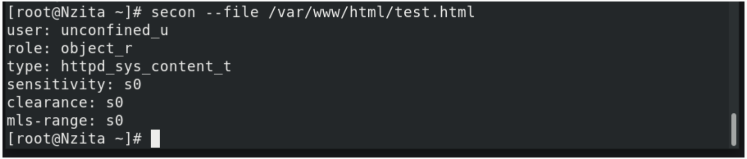
Рис. 8: Просмотр типов директорий в /var/www

Практическое знакомтсво с технологией SELinux



```
  GNU nano 2.9.8              /var/www/html/test.html              Modified

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

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

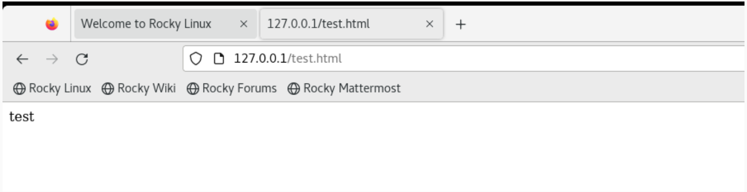
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# secon --file /var/www/html/test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[root@Nzita ~]# 
```

Рис. 10: Установка пароля для пользователя с правами администратора

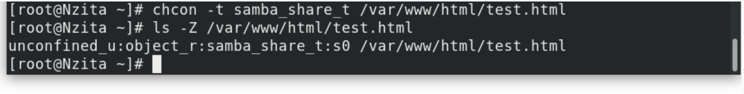
Практическое знакомтсво с технологией SELinux



test

Рис. 11: Открытие html-страницы через браузер

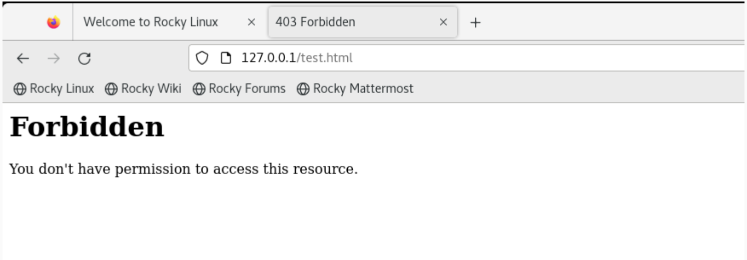
Практическое знакомтсво с технологией SELinux



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

Рис. 12: Изменение контекста файла /var/www/html/test.html

Практическое знакомтсво с технологией SELinux

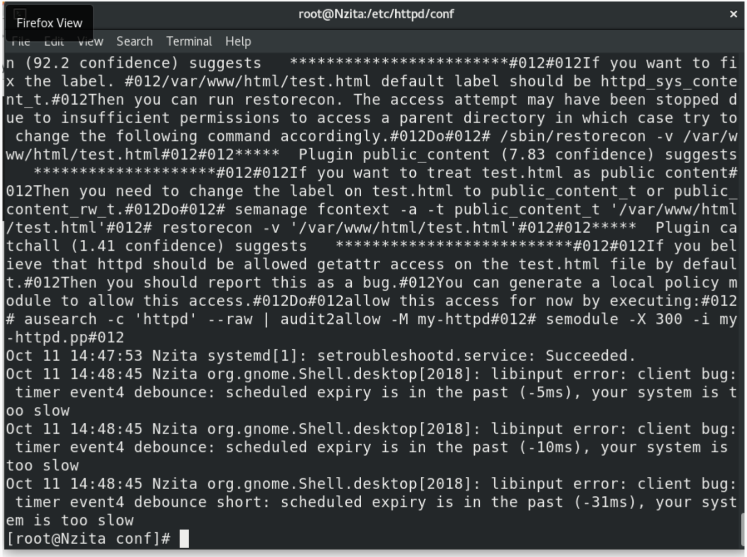


Forbidden

You don't have permission to access this resource.

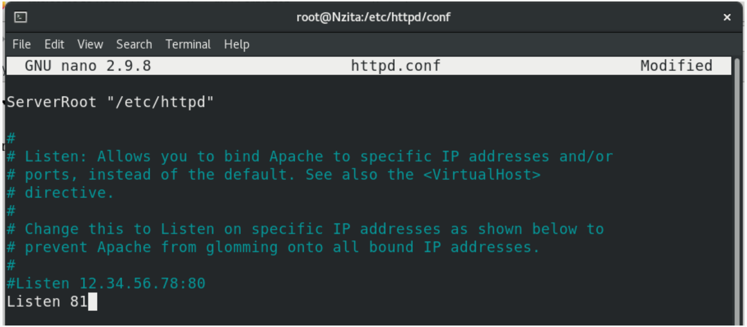
Рис. 13: Отказ в доступе к html-странице через браузер

Практическое знакомтсво с технологией SELinux


Firefox View
root@Nzita:/etc/httpd/conf
File Edit View Search Terminal Help

```
n (92.2 confidence) suggests   ***********************#012#012If you want to fi
x the label. #012/var/www/html/test.html default label should be httpd_sys_conte
nt_t.#012Then you can run restorecon. The access attempt may have been stopped d
ue to insufficient permissions to access a parent directory in which case try to
 change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/w
ww/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 ca
tchall (1.41 confidence) suggests   **************************#012#012If you bel
ieve that httpd should be allowed getattr access on the test.html file by defaul
t.#012Then you should report this as a bug.#012You can generate a local policy m
odule to allow this access.#012Do#012allow this access for now by executing:#012
# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my
-httpd.pp#012
Oct 11 14:47:53 Nzita systemd[1]: setroubleshootd.service: Succeeded.
Oct 11 14:48:45 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce: scheduled expiry is in the past (-5ms), your system is t
oo slow
Oct 11 14:48:45 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce: scheduled expiry is in the past (-10ms), your system is
too slow
Oct 11 14:48:45 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce short: scheduled expiry is in the past (-31ms), your syst
em is too slow
[root@Nzita conf]# 
```

Практическое знакомтсво с технологией SELinux

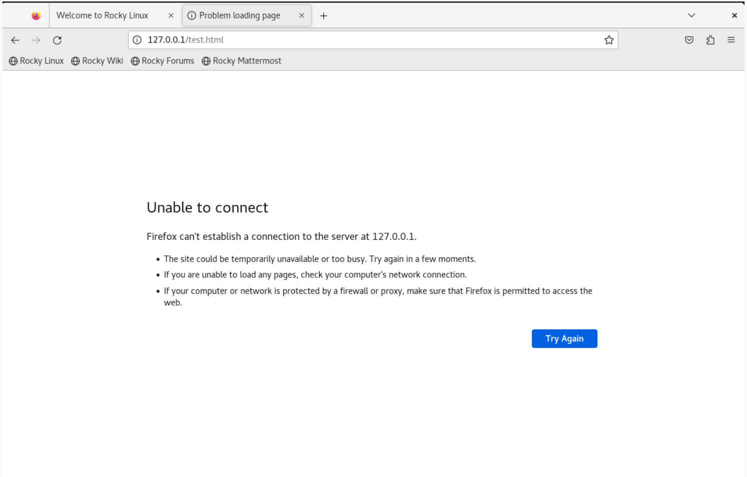


root@Nzita:/etc/httpd/conf
File Edit View Search Terminal Help

```
  GNU nano 2.9.8                 httpd.conf                Modified

ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 15: Замена прослушиваемого порта

Практическое знакомтсво с технологией SELinux



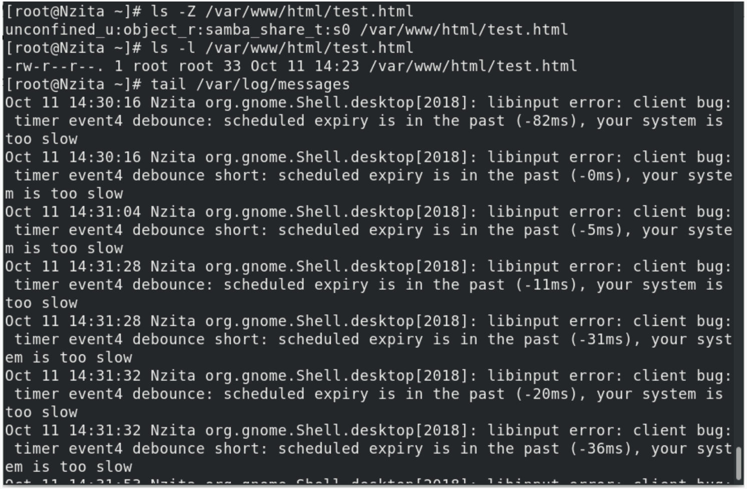
Unable to connect

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. 16: Открытие html-страницы через браузер при прослушивании 81 порта

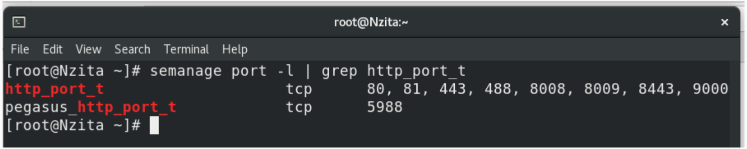
Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@Nzita ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct 11 14:23 /var/www/html/test.html
[root@Nzita ~]# tail /var/log/messages
Oct 11 14:30:16 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce: scheduled expiry is in the past (-82ms), your system is
too slow
Oct 11 14:30:16 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce short: scheduled expiry is in the past (-0ms), your syste
m is too slow
Oct 11 14:31:04 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce short: scheduled expiry is in the past (-5ms), your syste
m is too slow
Oct 11 14:31:28 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce: scheduled expiry is in the past (-11ms), your system is
too slow
Oct 11 14:31:28 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce short: scheduled expiry is in the past (-31ms), your syst
em is too slow
Oct 11 14:31:32 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce: scheduled expiry is in the past (-20ms), your system is
too slow
Oct 11 14:31:32 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
 timer event4 debounce short: scheduled expiry is in the past (-36ms), your syst
em is too slow
Oct 11 14:31:53 Nzita org.gnome.Shell.desktop[2018]: libinput error: client bug:
```

Рис. 17: Просмотр лог-файлов

Практическое знакомтсво с технологией SELinux



```
[root@Nzita ~]# 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@Nzita ~]# 
```

Рис. 18: Просмотр портов с помощью seamnage

Заключение

Выводы

В результате выполнения работы были приобретены практические навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работа SELinx на практике совместно с веб-сервером Apache.

Список литературы

SELinux – описание и особенности работы с системой. Часть 1 [Электронный ресурс]. Habr, 2014. URL: https://habr.com/ru/companies/kingservers/articles/209644/.