

Лабораторная работа №6

Мандатное разграничение прав в Linux

Парфенова Е. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньвна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

Важность понимания работы технологии SELinux для эффективной работы с ОС Linux и обеспечения директориям и файлам должной безопасности

Цель: Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Задача: Проверить работу SELinux на практике совместно с веб-сервером Apache.

Теоретическое введение

SELinux — это система принудительного контроля доступа, реализованная на уровне ядра, которая применяется только в том случае, если проверка классической системой прав Unix будет успешно пройдена.

Основные термины, использующиеся в SELinux:

- *Домен* — список действий, которые может выполнять процесс.
- *Роль* — список доменов, которые могут быть применены.
- *Тип* — набор действий, которые допустимы по отношению к объекту.
- *Контекст безопасности* — все атрибуты SELinux — роли, типы и домены.

SELinux имеет три основных режим работы, при этом по умолчанию установлен режим Enforcing. Режимы работы SELinux:

1. Enforcing
2. Permissive
3. Disabled

Выполнение лабораторной работы

```
[root@eeparfenova ~]# nano /etc/httpd/httpd.conf
[root@eeparfenova ~]# nano /etc/httpd/conf/httpd.conf
[root@eeparfenova ~]# iptables -F
[root@eeparfenova ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@eeparfenova ~]# iptables -P INPUT ACCEPT
[root@eeparfenova ~]# iptables -P OUTPUT ACCEPT
[root@eeparfenova ~]#
```

Рис. 1: Подготовка лабораторного стенда

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

Рис. 2: Просмотр режима и политики SELinux

Запуск и проверка работы сервера Apache

```
[eeparfenova@eeparfenova ~]$ su -
Password:
[root@eeparfenova ~]# 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: inactive (dead)
     Docs: man:httpd.service(8)
[root@eeparfenova ~]# sudo systemctl restart httpd
[root@eeparfenova ~]# sudo systemctl start httpd
[root@eeparfenova ~]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-10-09 17:56:00 MSK; 24s ago
     Docs: man:httpd.service(8)
  Main PID: 42967 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec:  0 B/sec"
    Tasks: 177 (limit: 12207)
   Memory: 24.0M
      CPU: 125ms
    CGroup: /system.slice/httpd.service
            └─42967 /usr/sbin/httpd -DFOREGROUND
              └─42968 /usr/sbin/httpd -DFOREGROUND
                └─42969 /usr/sbin/httpd -DFOREGROUND
                  └─42970 /usr/sbin/httpd -DFOREGROUND
                    └─42971 /usr/sbin/httpd -DFOREGROUND

Oct 09 17:56:00 eeparfenova.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 09 17:56:00 eeparfenova.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 09 17:56:00 eeparfenova.localdomain httpd[42967]: Server configured, listening on: port 80
[root@eeparfenova ~]#
```

Рис. 3: Запуск и проверка работы сервера Apache

Контекст безопасности сервера Apache: system_u:system_r:httpd_t:s0

```
[root@eeparfenova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 42967 0.0 0.5 20152 11544 ? Ss 17:55 0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42968 0.0 0.3 22032 7484 ? S 17:56 0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42969 0.0 0.6 1112588 13600 ? Sl 17:56 0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42970 0.0 0.6 981452 13412 ? Sl 17:56 0:00 /usr/sbin/http
d -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 42971 0.0 0.5 981452 11284 ? Sl 17:56 0:00 /usr/sbin/http
d -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 43203 0.0 0.1 221664 2304 pts/0 S+ 17:57 0:00 grep
--color=auto httpd
[root@eeparfenova ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 42967 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42968 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42969 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42970 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 42971 ? 00:00:00 httpd
[root@eeparfenova ~]#
```

Рис. 4: Контекст безопасности сервера Apache

Переключатели SELinux для Apache

```
(root@pearfenova ~)# 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_mysql off
httpd_can_connect_radius off
httpd_can_manage_courier_spool 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_avalahi off
httpd_dbus_ossd 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
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_tickshiff off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_ttp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_sasl off
httpd_verify_dns off
(root@pearfenova ~)#
```

Рис. 5: Текущее состояние переключателей SELinux для Apache


```
[root@eeparfenova ~]# 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:        65500  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 Constrai: 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
```

Рис. 6: Статистика по политике

Множество пользователей, ролей, типов

- Users - 8
- Roles - 15
- Types - 5145

```
[root@deeparfenova ~]# seinfo -u
users: 8
  guest_u
  root
  staff_u
  sysadm_u
  system_u
  unconfined_u
  user_u
  xguest_u
[root@deeparfenova ~]# 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@deeparfenova ~]# seinfo -t
Types: 5145
  NetworkManager_dispatcher_chronyc_script_t
  NetworkManager_dispatcher_chronyc_t
  NetworkManager_dispatcher_cloud_script_t
  NetworkManager_dispatcher_cloud_t
  NetworkManager_dispatcher_console_script_t
  NetworkManager_dispatcher_console_t
  NetworkManager_dispatcher_console_var_run_t
  NetworkManager_dispatcher_custom_t
  NetworkManager_dispatcher_ddclient_script_t
  NetworkManager_dispatcher_ddclient_t
  NetworkManager_dispatcher_dhclient_script_t
  NetworkManager_dispatcher_dhclient_t
  NetworkManager_dispatcher_dnsssec_script_t
  NetworkManager_dispatcher_dnsssec_t
```

Рис. 7: Множество пользователей, ролей, типов

```
[root@eeparfenova ~]# 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
[root@eeparfenova ~]# ls -lZ /var/www/html
total 0
[root@eeparfenova ~]#
```

Рис. 8: Файлы и поддиректори в /var/www

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

```
[root@deeparfenova ~]# nano /var/www/html/test.html  
[root@deeparfenova ~]# ls -lZ /var/www/html  
total 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct  9 18:07 test.html  
[root@deeparfenova ~]# ls -Z /var/www/html  
unconfined_u:object_r:httpd_sys_content_t:s0 test.html  
[root@deeparfenova ~]#
```

Рис. 9: Создание файла test.html и его контекст

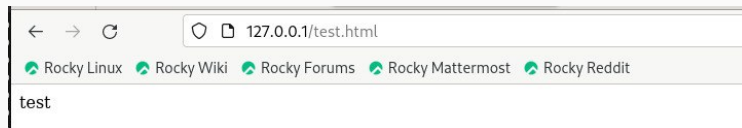


Рис. 10: Отображение файла через веб-сервер

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

Рис. 11: Изменение контекста файла

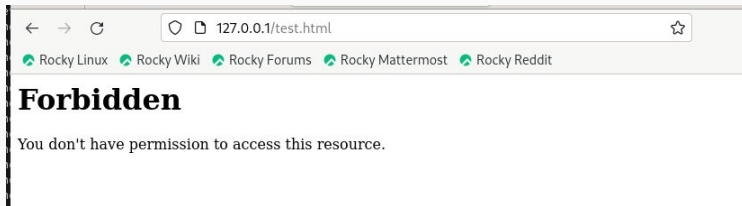


Рис. 12: Сообщение об ошибке после изменения контекста файла

```
#  
# 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 a specific IP address, but note that if  
# httpd.service is enabled to run at boot time, the address may not be  
# available when the service starts. See the httpd.service(8) man  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 81
```

Рис. 15: Замена порта в config файле

Сбой сервера при запуске с 81 порта

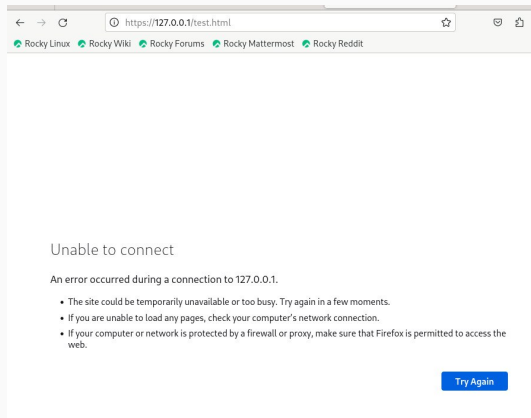


Рис. 16: Сбой сервера при запуске с 81 порта

Вывод: Появилась новая запись в лог-файла ошибок о невозможности загрузки, и не появилось новой записи в лог-файле доступа.

```
root@eeeparfenova ~]# tail -l /var/log/messages
Oct 9 18:32:48 eeeparfenova systemd[1]: Stopped The Apache HTTP Server.
Oct 9 18:32:48 eeeparfenova systemd[1]: httpd.service: Consumed 1.581s CPU time.
Oct 9 18:32:48 eeeparfenova systemd[1]: Starting The Apache HTTP Server...
Oct 9 18:32:48 eeeparfenova systemd[1]: Started The Apache HTTP Server.
Oct 9 18:32:48 eeeparfenova httpd[45113]: Server configured, listening on: port 81
Oct 9 18:34:34 eeeparfenova systemd[1646]: Started dbus-1.2-org.gnome.Screenshot@18.service.
Oct 9 18:34:41 eeeparfenova systemd[1]: Starting Hostname Service...
Oct 9 18:34:41 eeeparfenova systemd[1]: Started Hostname Service.
Oct 9 18:35:01 eeeparfenova systemd[1]: packagekit.service: Deactivated successfully.
Oct 9 18:35:01 eeeparfenova systemd[1]: packagekit.service: Consumed 1.208s CPU time.
```

Рис. 17: Файл /var/log/messages

Вывод: Страницы недоступна из-за неправильного контекста

```
[root@eeparfenova ~]# 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@eeparfenova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@eeparfenova ~]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@eeparfenova ~]# 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
[root@eeparfenova ~]#
```

Рис. 18: Добавление 81 порта

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

Рис. 19: Изменение контекста обратно

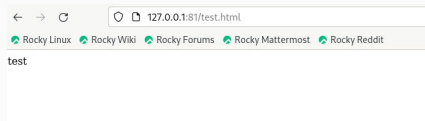


Рис. 20: Содержимое файла по новому адресу

```
[root@eeparfenova ~]# nano /etc/httpd/conf/httpd.conf
[root@eeparfenova ~]# semanage port -d -t http_port_t -p tcp 81
[root@eeparfenova ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@eeparfenova ~]# 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@eeparfenova ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@eeparfenova ~]#
```

Рис. 21: Возвращение всех изменений

Вывод

Мы развили навыки администрирования ОС Linux и получили первое практическое знакомство с технологией SELinux. Для этого мы проверили работу SELinux на практике совместно с веб-сервером Apache.