

Лабораторная работа №6

Мандатное разграничение прав в Linux

Голощапова Ирина Борисовна

14 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Голощапова Ирина Борисовна
- студентка уч. группы НФИбд-01-20
- Российский университет дружбы народов
- 1032201666@pfur.ru
- <https://github.com/ibgoloshchapowa>

Вводная часть

- Разграничение прав в Linux
- Дистрибутив Rocky
- Дискреционное разграничение доступа

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

Выполнение работы

Подготовка к выполнению работы

1. Установила от имени администратора httpd, задала параметр ServerName, также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp

```
servername test10
[root@ibgoloshchapowa conf]# cd
[root@ibgoloshchapowa ~]# iptables -F
[root@ibgoloshchapowa ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@ibgoloshchapowa ~]# iptables -P INPUT -p tcp --dport 80 -j ACCEPT
iptables v1.8.8 (nf_tables): -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.
[root@ibgoloshchapowa ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@ibgoloshchapowa ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@ibgoloshchapowa ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT
[root@ibgoloshchapowa ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT
[root@ibgoloshchapowa ~]#
```

Рис. 1: Отключение пакетного фильтра

Выполнение основной части работы

Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted

```
[guest2@ibgoloshchapowa ~]$ getenforce
Enforcing
[guest2@ibgoloshchapowa ~]$ setstatus
bash: setstatus: command not found...
[guest2@ibgoloshchapowa ~]$ 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
[guest2@ibgoloshchapowa ~]$
```

Рис. 2: Вход в систему

Выполнение основной части работы

Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает

```
[root@ibgoloshchapowa guest2]# 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; preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
lines 1-4/4 (END)
```

Рис. 3: Обращение к веб-браузеру

Выполнение основной части работы

Посмотрела текущее состояние переключателей SELinux для Apache

```
[root@hgoloshchapova guest2]# 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_idap          off
httpd_can_connect_mysql         off
httpd_can_connect_zabbix       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_avahi                off
httpd_dbus_aval                 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_windbind    off
httpd_mod_auth_pam              off
httpd_read_user_content         off
httpd_run_ipa                   off
httpd_run_preupgrade            off
httpd_run_ttkchshif            off
httpd_serve_cobbler_files       off
httpd_setrlimit                 off
httpd_ssl_exec                  off
httpd_vnc_script_anon_write     off
httpd_tty_exec                  off
httpd_tty_com                   off
httpd_unified                   off
httpd_use_cifs                  off
httpd_use_fusefs                off
httpd_use_egg                   off
httpd_use_nfs                   off
httpd_use_openscryptoki         off
httpd_use_opensstack            off
httpd_use_sasl                  off
httpd_verify_dns                off
[root@hgoloshchapova guest2]#
```

Рис. 4: переключатели SELinux

Выполнение основной части работы

Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов (рис. (fig:08?)):

```
httpd_verify_dns      off
[root@ibgoloshchapowa guest2]# 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:                 5100  Attributes:            258
Users:                 8     Roles:                 14
Booleans:              353   Cond. Expr.:          384
Allow:                 65000  Neverallow:            0
Auditallow:            170   Dontaudit:             8572
Type_trans:            265341  Type_change:           87
Type_member:           35     Range_trans:           6164
Role allow:            38     Role_trans:            420
Constraints:           70     Validatetrans:         0
MLS Constrain:         72     MLS Val. Tran:         0
Permissives:           2     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:               660
Netifcon:              0     Nodecon:               0
[root@ibgoloshchapowa guest2]#
```

Выполнение основной части работы

Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл следующего содержания



Рис. 6: html-файл

Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`

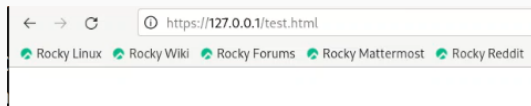
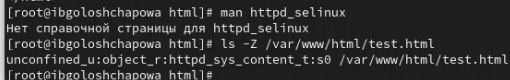


Рис. 7: Обращение к файлу через веб-сервер

Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd`. Сопоставила их с типом файла `test.html`. Проверила контекст файла командой `ls -Z`



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

Рис. 8: контексты файлов для `httpd`

Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`

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

Рис. 9: Изменение контекст файла

Выполнение основной части работы

Попробовала 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 нашла строчку Listen 80 и заменила её на Listen 81

```
40 #
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a DSO you
53 # have to place corresponding 'LoadModule' lines at this location so the
```

Рис. 10: Замена на Listen 81

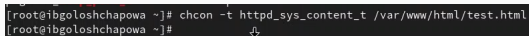
Выполнение основной части работы

Выполнила команду и после этого проверила список портов

```
[root@ibgoloshchapowa ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@ibgoloshchapowa ~]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 900
0
pegasus_http_port_t  tcp      5988
[root@ibgoloshchapowa ~]#
```

Рис. 11: Список портов

Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` и после этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`

A terminal window with a dark background. The prompt is [root@ibgoloshchapowa ~]#. The command entered is chcon -t httpd_sys_content_t /var/www/html/test.html. The prompt on the next line is [root@ibgoloshchapowa ~]#.

```
[root@ibgoloshchapowa ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ibgoloshchapowa ~]#
```

Рис. 12: Возврат контекст

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту и проверила, что порт 81 удалён. Затем удалила файл /var/www/html/test.html

```
[root@ibgoloshchapova ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ibgoloshchapova ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@ibgoloshchapova ~]#
```

Рис. 13: Удаление привязки и файла

В ходе лабораторной работы мне удалось:

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