

Информационная безопасность

Л.6. Мандатное разграничение прав в Linux

Греков Максим Сергеевич

2021

Содержание

1	Цель работы	4
2	Подготовка лабораторного стенда	5
2.1	ServerName	5
2.2	Пакетный фильтр	5
3	Порядок выполнения работы	6
3.1	Режим SELinux	6
3.2	Рабочий веб-сервер	6
3.3	Веб-сервер Apache	7
3.4	Переключатели SELinux для Apache	7
3.5	Команда seinfo	8
3.6	Тип файлов и поддиректорий www	9
3.7	Тип файлов и поддиректорий html	9
3.8	Создание файлов в директории html	9
3.9	Создание test.html	10
3.10	Проверка контекста	11
3.11	Файл из браузера и справка	11
3.12	Изменение контекста	11
3.13	Доступ к файлу	12
3.14	Log-файлы веб-сервера Apache	12
3.15	Прослушивание TCP-порта 81	13
3.16	Анализ файлов	13
3.17	Добавление порта 81	13
3.18	Возврат контекста	14
3.19	Откат изменений	14
4	Вывод	15

List of Figures

2.1	ServerName	5
2.2	Пакетный фильтр	5
3.1	Режим SELinux	6
3.2	Рабочий веб-сервер	7
3.3	Веб-сервер Apache	7
3.4	Переключатели SELinux для Apache	8
3.5	Команда seinfo	8
3.6	Тип файлов и поддиректорий www	9
3.7	Тип файлов и поддиректорий www	9
3.8	Тип файлов и поддиректорий www	10
3.9	Создание test.html	10
3.10	Проверка контекста	11
3.11	Изменение контекста	11
3.12	Доступ к файлу	12
3.13	Log-файлы веб-сервера Apache	12
3.14	Прослушивание TCP-порта 81	13
3.15	Анализ файлов	13
3.16	Добавление порта 81	14
3.17	Откат изменений	14

1 Цель работы

Развить навыки администрирования ОС Linux.

Получить первое практическое знакомство с технологией SELinux.

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

2 Подготовка лабораторного стенда

2.1 ServerName

В конфигурационном файле `/etc/httpd/httpd.conf` задали параметр `ServerName` (рис. 2.1): `ServerName test.ru`

Это нужно для того, чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.

```
[root@grekovms etc]# cd httpd
[root@grekovms httpd]# ls
conf  conf.d  conf.modules.d  logs  modules  run  state
[root@grekovms httpd]# echo "ServerName test.ru" >> httpd.conf
```

Figure 2.1: ServerName

2.2 Пакетный фильтр

Проследили, чтобы пакетный фильтр был отключён, для этого воспользовались командами (рис. 2.2):

- `iptables -F`
- `iptables -P INPUT ACCEPT`
- `iptables -P OUTPUT ACCEPT`

```
[root@grekovms httpd]# iptables -F
[root@grekovms httpd]# iptables -P INPUT ACCEPT
[root@grekovms httpd]# iptables -P OUTPUT ACCEPT
[root@grekovms httpd]#
```

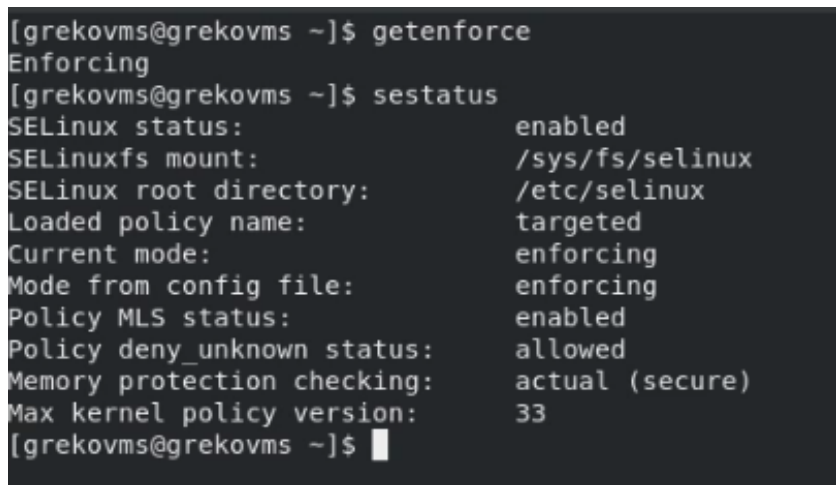
Figure 2.2: Пакетный фильтр

3 Порядок выполнения работы

3.1 Режим SELinux

Вошли в систему со своими учётными данными и убедитесь (рис. 3.1), что SELinux работает в режиме *enforcing* политики *targeted* с помощью команд:

- `getenforce`
- `sestatus`

A terminal window showing the output of the 'getenforce' and 'sestatus' commands. The 'getenforce' command returns 'Enforcing'. The 'sestatus' command provides a detailed status report for SELinux, including its enabled state, file system mounts, root directory, loaded policy name, current mode, and other configuration details.

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

Figure 3.1: Режим SELinux

3.2 Рабочий веб-сервер

Обратились через терминал к веб-серверу (рис. 3.2), запущенному на компьютере, и убедились, что последний работает:

- service httpd status
- /etc/rc.d/init.d/httpd status

```
[grekovms@grekovms ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 19:04:52 MSK; 40s ago
     Docs: man:httpd.service(8)
  Main PID: 41141 (httpd)
    Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 5039)
   Memory: 21.6M
    CGroup: /system.slice/httpd.service
            └─41141 /usr/sbin/httpd -DFOREGROUND
              └─41148 /usr/sbin/httpd -DFOREGROUND
                └─41149 /usr/sbin/httpd -DFOREGROUND
                  └─41150 /usr/sbin/httpd -DFOREGROUND
                    └─41151 /usr/sbin/httpd -DFOREGROUND

ноя 27 19:04:51 grekovms.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 19:04:52 grekovms.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 19:04:52 grekovms.localdomain httpd[41141]: Server configured, listening on: port 80
```

Figure 3.2: Рабочий веб-сервер

3.3 Веб-сервер Apache

Нашли веб-сервер Apache (рис. 3.3) в списке процессов, определили его контекст безопасности:

- ps auxZ | grep httpd

```
[grekovms@grekovms ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 41141 0.0 1.2 282900 12016 ? Ss 19:04
:04 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41148 0.0 0.8 296780 8596 ? S 19:04
:04 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41149 0.0 1.2 1485696 12412 ? Sl 19:04
:04 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41150 0.0 1.0 1354568 10372 ? Sl 19:04
:04 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41151 0.0 1.0 1354568 10372 ? Sl 19:04
:04 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 grekovms 41461 0.0 0.1 12136 1188
pts/0 R+ 19:06 0:00 grep --color=auto httpd
[grekovms@grekovms ~]$
```

Figure 3.3: Веб-сервер Apache

3.4 Переключатели SELinux для Apache

Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды:

- `sestatus -bigrep httpd`

Обратили внимание (рис. 3.4), что многие из них находятся в положении «off»:

```
[grekovms@grekovms etc]$ 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 off
httpd_manage_ipa off
```

Figure 3.4: Переключатели SELinux для Apache

3.5 Команда `seinfo`

Посмотрели статистику по политике с помощью команды `seinfo` (рис. 3.5), также определили множество пользователей, ролей, типов:

```
[grekovms@grekovms ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 463
Sensitivities: 1 Categories: 1024
Types: 4959 Attributes: 255
Users: 8 Roles: 14
Booleans: 340 Cond. Expr.: 389
Allow: 112885 Neverallow: 0
Auditallow: 166 Dontaudit: 10362
Type trans: 253398 Type change: 87
Type member: 35 Range trans: 6015
Role allow: 38 Role trans: 423
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: 33
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0
```

Figure 3.5: Команда `seinfo`

3.6 Тип файлов и поддиректорий `www`

Определили тип файлов и поддиректорий (рис. 3.6), находящихся в директории `/var/www`, с помощью команды:

- `ls -lZ /var/www`

```
[grekovms@grekovms ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58
cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58
html
```

Figure 3.6: Тип файлов и поддиректорий `www`

3.7 Тип файлов и поддиректорий `html`

Определили тип файлов (рис. 3.7), находящихся в директории `/var/www/html` с помощью команды:

- `ls -lZ /var/www/html`

Убедились, что файлы отсутствуют.

```
[grekovms@grekovms ~]$ ls -lZ /var/www/html
итого 0
[grekovms@grekovms ~]$
```

Figure 3.7: Тип файлов и поддиректорий `www`

3.8 Создание файлов в директории `html`

Определили круг пользователей (рис. 3.8), которым разрешено создание файлов в директории `/var/www/html` - пользователи с `root` правами:

```

[grekovms@grekovms /]$ ls -lZ /var/www/html
итого 0
[grekovms@grekovms /]$ touch a.txt
touch: невозможно выполнить touch для 'a.txt': Отказано в доступе
[grekovms@grekovms /]$ su root
Пароль:
[root@grekovms /]# cd var/www
[root@grekovms www]# ls
cgi-bin  html
[root@grekovms www]# cd html
[root@grekovms html]# ls
[root@grekovms html]# touch a.txt
[root@grekovms html]# ls
a.txt

```

Figure 3.8: Тип файлов и поддиректорий www

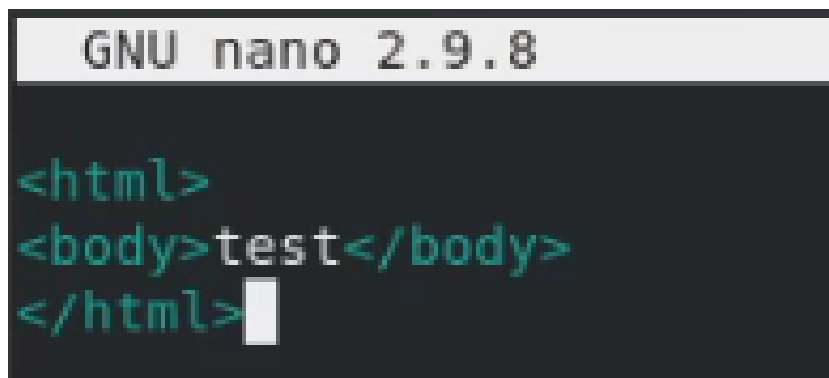
3.9 Создание test.html

Создали от имени суперпользователя html-файл `/var/www/html/test.html` (рис. 3.9) следующего содержания:

```

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

```



```

GNU nano 2.9.8

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

```

Figure 3.9: Создание test.html

3.10 Проверка контекста

Проверили контекст созданного файла и контекст, присваиваемый по умолчанию (рис. 3.10) вновь созданным файлам в директории `/var/www/html`:

```
[root@grekovms html]# ls -lZ
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0
test.html
[root@grekovms html]#
```

Figure 3.10: Проверка контекста

3.11 Файл из браузера и справка

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

Убедились, что файл был успешно отображён.

Изучили справку `man httpd_selinux` и выяснили, какие контексты файлов определены для `httpd`.

3.12 Изменение контекста

Изменили контекст файла `/var/www/html/test.html` (рис. 3.11) с `httpd_sys_content_t` на `samba_share_t`, к которому процесс `httpd` не должен иметь доступа, и проверили, что он поменялся:

- `chcon -t samba_share_t /var/www/html/test.html`
- `ls -Z /var/www/html/test.html`

```
[root@grekovms html]# chcon -t samba_share_t test.html
[root@grekovms html]# ls -Z test.html
unconfined_u:object_r:samba_share_t:s0 test.html
[root@grekovms html]#
```

Figure 3.11: Изменение контекста

3.13 Доступ к файлу

Попробовали получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`, и получили сообщение об ошибке.

Хоть права доступа и позволяют читать этот файл любому пользователю (рис. 3.12), однако из-за контекста файл нет был отображён.

- `ls -l /var/www/html/test.html`

```
[root@grekovms html]# ls -l test.html
-rw-r--r--. 1 root root 33 ноя 27 18:52 test.html
[root@grekovms html]#
```

Figure 3.12: Доступ к файлу

3.14 Log-файлы веб-сервера Apache

Просмотрели log-файлы веб-сервера Apache, также просмотрели системный лог-файл (рис. 3.13):

- `tail /var/log/messages`

```
[root@grekovms /]# tail /var/log/messages
Nov 27 19:16:42 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: last use
r_time (5742268) is greater than comparison timestamp (5741964). This most likely repre
sents a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDO
W. Trying to work around...
Nov 27 19:16:42 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: W12 appe
ars to be one of the offending windows with a timestamp of 5742268. Working around...
Nov 27 19:18:55 grekovms dbus-daemon[843]: [system] Activating via systemd: service name
='net.reactivated.Fprint' unit='fprintd.service' requested by ':l.677' (uid=0 pid=42365
comm="su root " label="unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023")
Nov 27 19:18:55 grekovms systemd[1]: Starting Fingerprint Authentication Daemon...
Nov 27 19:18:56 grekovms dbus-daemon[843]: [system] Successfully activated service 'net.
reactivated.Fprint'
Nov 27 19:18:56 grekovms systemd[1]: Started Fingerprint Authentication Daemon.
Nov 27 19:18:57 grekovms su[42365]: (to root) grekovms on pts/0
Nov 27 19:19:26 grekovms systemd[1]: fprintd.service: Succeeded.
Nov 27 19:22:15 grekovms org.gnome.Shell.desktop[1815]: libinput error: client bug: time
r event3 debounce: scheduled expiry is in the past (-143ms), your system is too slow
Nov 27 19:22:15 grekovms org.gnome.Shell.desktop[1815]: libinput error: client bug: time
r event3 debounce short: scheduled expiry is in the past (-156ms), your system is too sl
ow
```

Figure 3.13: Log-файлы веб-сервера Apache

3.15 Прослушивание TCP-порта 81

Попробовали запустить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 3.14) (а не 80, как рекомендует IANA и прописано в `/etc/services`).

Для этого в файле `/etc/httpd/httpd.conf` нашли строчку `Listen 80` и заменили её на `Listen 81`, потом выполнили перезапуск сервера.

```
# prevent Apache from glomming onto all b
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
```

Figure 3.14: Прослушивание TCP-порта 81

3.16 Анализ файлов

Просмотрели (рис. 3.15) и проанализировали файлы `/var/log/messages`, `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`:

```
[root@grekovms log]# tail -n 10 messages
Nov 27 19:30:50 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: last user time (6589380) is greater than com
parison timestamp (6589380). This most likely represents a buggy client sending inaccurate timestamps in messages such as _
NET ACTIVE WINDOW. Trying to work around...
Nov 27 19:30:50 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: W12 appears to be one of the offending windo
ws with a timestamp of 6589381. Working around...
Nov 27 19:30:50 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: last user time (6589717) is greater than com
parison timestamp (6589716). This most likely represents a buggy client sending inaccurate timestamps in messages such as _
NET ACTIVE WINDOW. Trying to work around...
Nov 27 19:30:50 grekovms org.gnome.Shell.desktop[1815]: Window manager warning: W12 appears to be one of the offending windo
ws with a timestamp of 6589717. Working around...
Nov 27 19:33:26 grekovms systemd[1]: Stopping The Apache HTTP Server...
Nov 27 19:33:28 grekovms systemd[1]: httpd.service: Succeeded.
Nov 27 19:33:28 grekovms systemd[1]: Stopped The Apache HTTP Server.
Nov 27 19:33:28 grekovms systemd[1]: Starting The Apache HTTP Server...
Nov 27 19:33:29 grekovms systemd[1]: Started The Apache HTTP Server.
Nov 27 19:33:29 grekovms httpd[42774]: Server configured, listening on: port 81
[root@grekovms log]# cd ...
```

Figure 3.15: Анализ файлов

3.17 Добавление порта 81

Выполнили команду `semanage port -a -t http_port_t -p tcp 81` (рис. 3.16)

После этого проверили список портов командой `semanage port -l | grep http_port_t` и убедились, что порт 81 появился в списке, затем выполнили перезапуск сервера.

```
[root@grekovms /]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@grekovms /]# 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@grekovms /]#
```

Figure 3.16: Добавление порта 81

3.18 Возврат контекста

Вернули 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 попробовали получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`, увидели его содержимое.

3.19 Откат изменений

- Исправили обратно конфигурационный файл `apache`, вернув `Listen 80`.
- Удалили привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` (рис. 3.17)
- Удалили файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
IncludeOptional conf.d/*.conf
[root@grekovms /]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@grekovms /]# cd
[root@grekovms ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg
[root@grekovms ~]# cd ..
[root@grekovms /]# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin
[root@grekovms /]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
```

Figure 3.17: Откат изменений

4 Вывод

Развили навыки администрирования ОС Linux.

Получили первое практическое знакомство с технологией SELinux.

Проверили работу SELinux на практике совместно с веб-сервером Apache.