

Презентация по лабараторной работе №6

Кучен Ирзилей Сайын НФИбд-03-18

1. Цель и задачи

- Цель лабораторной работы --- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.
- Выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт.

Ход работы

• 1.

The screenshot displays a virtual machine environment with two main windows. The left window is a PDF viewer showing a document titled '006-lab_selinux.pdf'. The right window is a terminal window titled 'Base [Работает] - Oracle VM VirtualBox'.

PDF Document Content:

кон консолиной программой будет производиться подключение к веб-серверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

6.4. Порядок выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:
`service httpd status`
или
`/etc/rc.d/init.d/httpd status`
Если не работает, запустите его так же, но с параметром `start`.
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду
`ps auxZ | grep httpd`
или
`ps -eZ | grep httpd`
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды
`sestatus -bigrep httpd`
Обратите внимание, что многие из них находятся в положении «off».

42 Кулябов Д. С., Королькова А. В., Геворкян М. Н.

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды
`ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`:
`ls -lZ /var/www/html`
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.

Terminal Window Content:

```
irziley@localhost:~$ setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
[irziley@localhost ~]$ getenforce
Enforcing
[irziley@localhost ~]$ setstatus
bash: setstatus: команда не найдена...
[irziley@localhost ~]$ 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
[irziley@localhost ~]$
```

2.

The screenshot displays a virtual machine environment with two main windows:

PDF Document (006-lab_selinux.pdf):

2 / 5 | 100%

кон консолиной программой) будет производиться подключение к веб-серверу. По желанию могут использоваться разные программы, такие как консольные `links`, `lynx`, `wget` и графические `konqueror`, `opera`, `firefox` или др.

6.4. Порядок выполнения работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:
`service httpd status`
или
`/etc/rc.d/init.d/httpd status`
Если не работает, запустите его так же, но с параметром `start`.
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду
`ps auxZ | grep httpd`
или
`ps -eZ | grep httpd`
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды
`sestatus -bigrep httpd`
Обратите внимание, что многие из них находятся в положении «off».

42 Кулябов Д. С., Королькова А. В., Геворкян М. Н.

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды
`ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`:
`ls -lZ /var/www/html`
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.

Terminal Window (Terminal):

irziley@localhost:~

```
[irziley@localhost ~]$ getenforce
Enforcing
[irziley@localhost ~]$ 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
[irziley@localhost ~]$ 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: enabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
lines 1-4/4 (END)
```

The bottom of the image shows the Windows taskbar with the search bar containing "Введите здесь текст для поиска", system tray icons, and the date/time "19:23 27.11.2021".

3.

The screenshot shows a Windows 10 desktop with two main windows. The left window is a web browser displaying a PDF document titled '006-lab_selinux.pdf'. The right window is a terminal window titled 'Base [Работает] - Oracle VM VirtualBox' showing a Linux shell prompt 'irziley@localhost:~'.

Web Browser Window:

- Address bar: `esystem.rudn.ru/pluginfile.php/1198119/mod_...`
- PDF Title: `006-lab_selinux.pdf`
- Page: `2 / 5`
- Zoom: `100%`

PDF Content:

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:
`service httpd status`
или
`/etc/rc.d/init.d/httpd status`
Если не работает, запустите его так же, но с параметром `start`.
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду
`ps auxZ | grep httpd`
или
`ps -eZ | grep httpd`
4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды
`sestatus -bigrep httpd`
Обратите внимание, что многие из них находятся в положении «off».

Terminal Window:

```
irziley@localhost:~$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 irziley 8839 0.0  0.0 1213
6 1036 pts/0 R+  11:24   0:00 grep --color=auto httpd
irziley@localhost ~]$ ps -eZ | grep httpd
irziley@localhost ~]$ H
```

Taskbar:

- Search: `Введите здесь текст для поиска`
- System tray: `100%`, `1°C`, `ENG`, `19:24`, `27.11.2021`

4.

The screenshot displays a virtual machine environment with two main windows:

PDF Document (006-lab_selinux.pdf):

- Page 3:**
 - Если не работает, запустите его так же, но с параметром `start`.
 - 3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`.
 - 4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`. Обратите внимание, что многие из них находятся в положении «off».
- Page 42:**
 - 5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
 - 6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`.
 - 7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`.
 - 8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
 - 9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания:


```
<html>
<body>test</body>
</html>
```
 - 10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
 - 11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.
 - 12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`.

Terminal Window (irziley@localhost):

```
[irziley@localhost ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 irziley 8839 0.0  0.0 1213
6 1036 pts/0 R+ 11:24  0:00 grep --color=auto httpd
[irziley@localhost ~]$ ps -eZ | grep httpd
[irziley@localhost ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[irziley@localhost ~]$
```

The terminal window shows the output of the `ps auxZ | grep httpd` command, which displays the SELinux context for the `httpd` process. The output indicates that the process is running with the context `unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023`. The `sestatus -bigrep httpd` command is also shown, but it results in an error: `sestatus: invalid option -- 'i'`.

5.

Family Guy | Course: Инф... | Лабораторн... | 006-lab_selin...

esystem.rudn.ru/pluginfile.php/1198119/mod_...

Сервисы | American Center in... | Immigration Matter... | Free Text to Speech... | Список для чтения...

006-lab_selinux.pdf | 3 / 5 | 100%

42 Кулябов Д. С., Королькова А. В., Геворкян М. Н.

- Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
- Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
- Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`
- Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
- Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) `html`-файл `/var/www/html/test.html` следующего содержания:


```
<html>
<body>test</body>
</html>
```
- Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
- Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.
- Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`.


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

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.

Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к фай-

Base [Работает] - Oracle VM VirtualBox

Файл | Машина | Вид | Ввод | Устройства | Справка

Обзор | Терминал | C6, 27 ноября 11:26 | en

irziley@localhost:~

Файл | Правка | Вид | Поиск | Терминал | Справка

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:	112894	Neverallow:	0
Auditallow:	166	Dontaudit:	10362
Type_trans:	253622	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

[irziley@localhost ~]\$

100% | 19:26 | 27.11.2021

6.

Family Guy Sl x Course: Инф x Лабораторн x 006-lab_selin x +

esystem.rudn.ru/pluginfile.php/1198119/mod_...

Сервисы American Center in... Immigration Matter... Free Text to Speech... Списание для чтения

006-lab_selinux.pdf 3 / 5 100%

42 Кулябов Д. С., Королькова А. В., Геворкян М. Н.

- Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
- Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
- Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`
- Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
- Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директории) `html`-файл `/var/www/html/test.html` следующего содержания:


```
<html>
<body>test</body>
</html>
```
- Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
- Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.
- Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`.


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

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.

Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к фай-

Base [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал C6, 27 ноября 11:27 en

irziley@localhost:~

Файл Правка Вид Поиск Терминал Справка

Auditallow:	166	Dontaudit:	10362
Type_trans:	253622	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

```
[irziley@localhost ~]$ ls -lZ /var/www
ls: неверный ключ - «Z»
По команде «ls --help» можно получить дополнительную информацию.
[irziley@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 11 23
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 11 23
:58 html
[irziley@localhost ~]$
```

100% 1°C 19:27 27.11.2021

7.

The screenshot shows a virtual machine environment with two main windows:

Web Browser Window (Left)

Address bar: `esystem.rudn.ru/pluginfile.php/1198119/mod_...`

Document title: `006-lab_selinux.pdf`

Page: 3 / 5, 100% zoom

Content of the PDF (Task 13):

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

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

Terminal Window (Right)

Host: `irziley@localhost:~`

Commands and output:

```
[irziley@localhost ~]$ ls -lZ /var/www
ls: неверный ключ - «Z»
По команде «ls --help» можно получить дополнительную информацию.
[irziley@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 11 23
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 11 23
:58 html
[irziley@localhost ~]$ ls -lZ /var/www/html
итого 0
[irziley@localhost ~]$
```

System tray at the bottom shows the date and time: 19:27 27.11.2021.

8.

The screenshot displays a virtual machine environment with two main windows:

- PDF Document (006-lab_selinux.pdf):** This window shows a list of tasks for a SELinux lab. The tasks are numbered 5 through 13. Task 13 involves changing the context of a file from `httpd_sys_content_t` to `samba_share_t` using the `chcon` command.
- Terminal Window:** This window shows the execution of several commands in a Linux environment. The commands and their outputs are as follows:
 - `ls -lZ /var/www`: Output shows permissions for `cgi-bin` and `html` directories.
 - `ls -lZ /var/www/html`: Output shows permissions for files in the `html` directory.
 - `ls -lZ /var/www/html/test.html`: Output shows the context of the `test.html` file.

The bottom of the image shows the Windows taskbar with various application icons and system status indicators.

9.

The screenshot displays a virtual machine environment with two main windows. The left window is a web browser showing a PDF document titled '006-lab_selinux.pdf'. The right window is a file manager showing the contents of the 'Рабочий стол' (Desktop) directory.

Web Browser Window:

- Address bar: `esystem.rudn.ru/pluginfile.php/1198119/mod_...`
- PDF Title: `006-lab_selinux.pdf`
- Page: 3 / 5
- Zoom: 100%

File Manager Window:

- Path: `Домашняя папка > Рабочий стол`
- Files and Folders:
 - `simpleid.c` (file)
 - `test.html` (file)
 - `Видео` (folder)
 - `Документы` (folder)
 - `Загрузки` (folder)
 - `Изображения` (folder)
 - `Музыка` (folder)
 - `Общедоступные` (folder)
 - `Рабочий стол` (folder)
 - `Шаблоны` (folder)

PDF Content (Page 3):

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

8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.

9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директории) `html`-файл `/var/www/html/test.html` следующего содержания:

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

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`.

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

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.

Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `:s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

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

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


10.

The screenshot displays a virtual machine environment with two main windows:

- Web Browser (Left):** The address bar shows `esystem.rudn.ru/pluginfile.php/1198119/mod_...`. The page content displays a PDF document titled `006-lab_selinux.pdf`. The document includes instructions for SELinux configuration, such as creating a file in `/var/www/html` and checking the context. The visible text includes:


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

 - Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`.
 - Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания:


```
<html>
<body>test</body>
</html>
```
 - Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
 - Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.
 - Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -lZ`.


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

 Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.
 Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `s0`).
 - Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.
 - Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`:


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

- Text Editor (Right):** The editor window is titled `test` and shows the following HTML content:


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

The bottom of the image shows the Windows taskbar with various application icons and system tray information, including the date `27.11.2021` and time `19:31`.

11.

The screenshot displays a virtual machine environment with two main windows. The left window is a PDF viewer showing a document titled '006-lab_selinux.pdf'. The right window is a web browser (Firefox) displaying a file named 'test' at the path 'file:///home/irziley/test.html'.

PDF Document Content:

ls -lZ /var/www/html

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.

9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

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

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -lZ`.

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

Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (`unconfined` в переводе с англ. означает свободный), созданному нами файлу `test.html` был сопоставлен SELinux, пользователь `unconfined_u`. Это первая часть контекста.

Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль `object_r` используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории `/proc` файлы, относящиеся к процессам, могут иметь роль `system_r`. Если активна политика MLS, то могут использоваться и другие роли, например, `secadm_r`. Данный случай мы рассматривать не будем, как и предназначение `s0`).

Тип `httpd_sys_content_t` позволяет процессу `httpd` получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

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

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

Web Browser Content:

Обзор Firefox С6, 27 ноября 11:32 en

/home/irziley/test.html

file:///home/irziley/test.html

test

Выводы

- В результате выполнения работы мы изучили развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.