Презентация по лабараторной работе №6

Кучен Ирзилей Сайын НФИбд-03-18

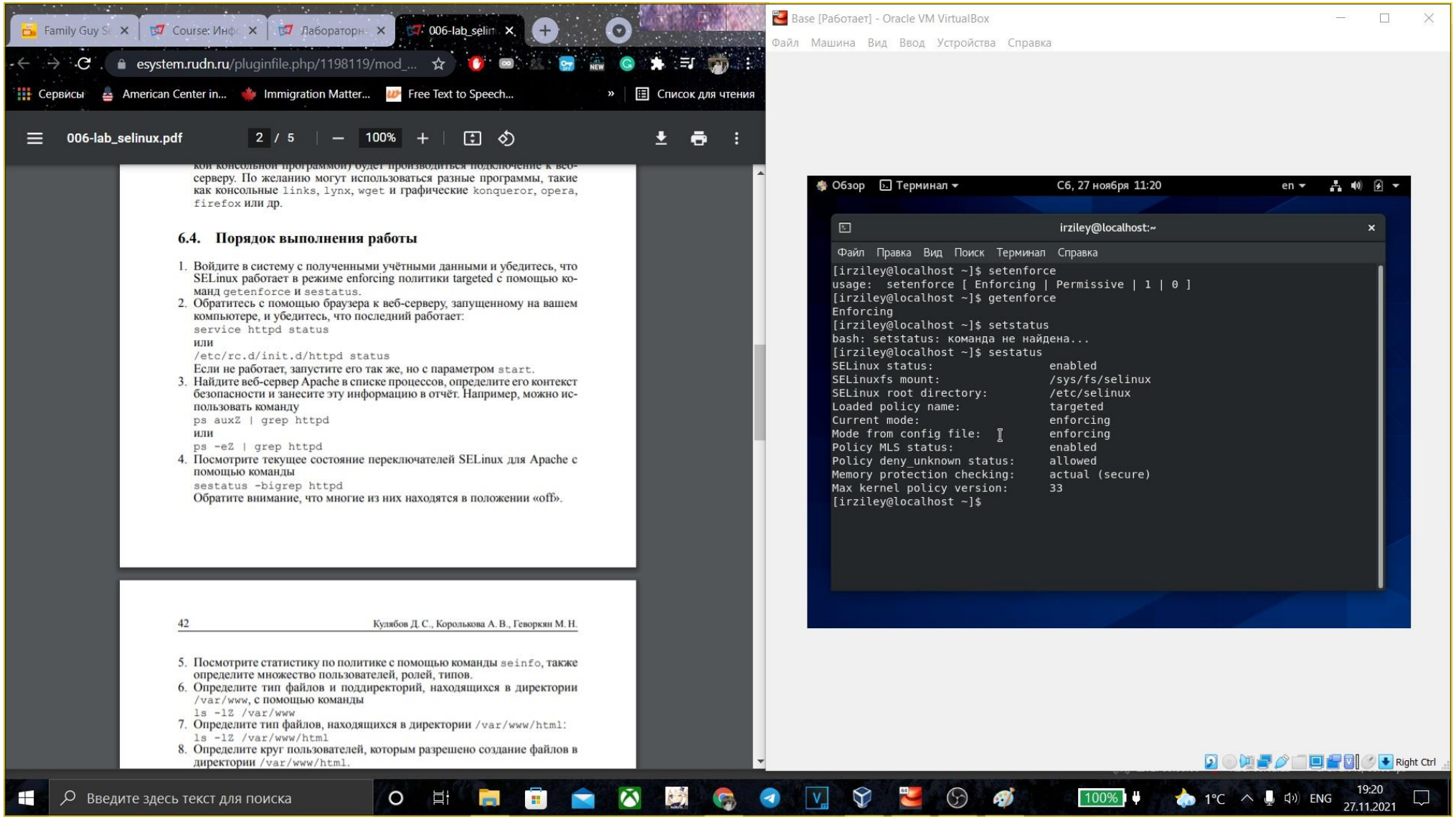
1. Цель и задачи

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

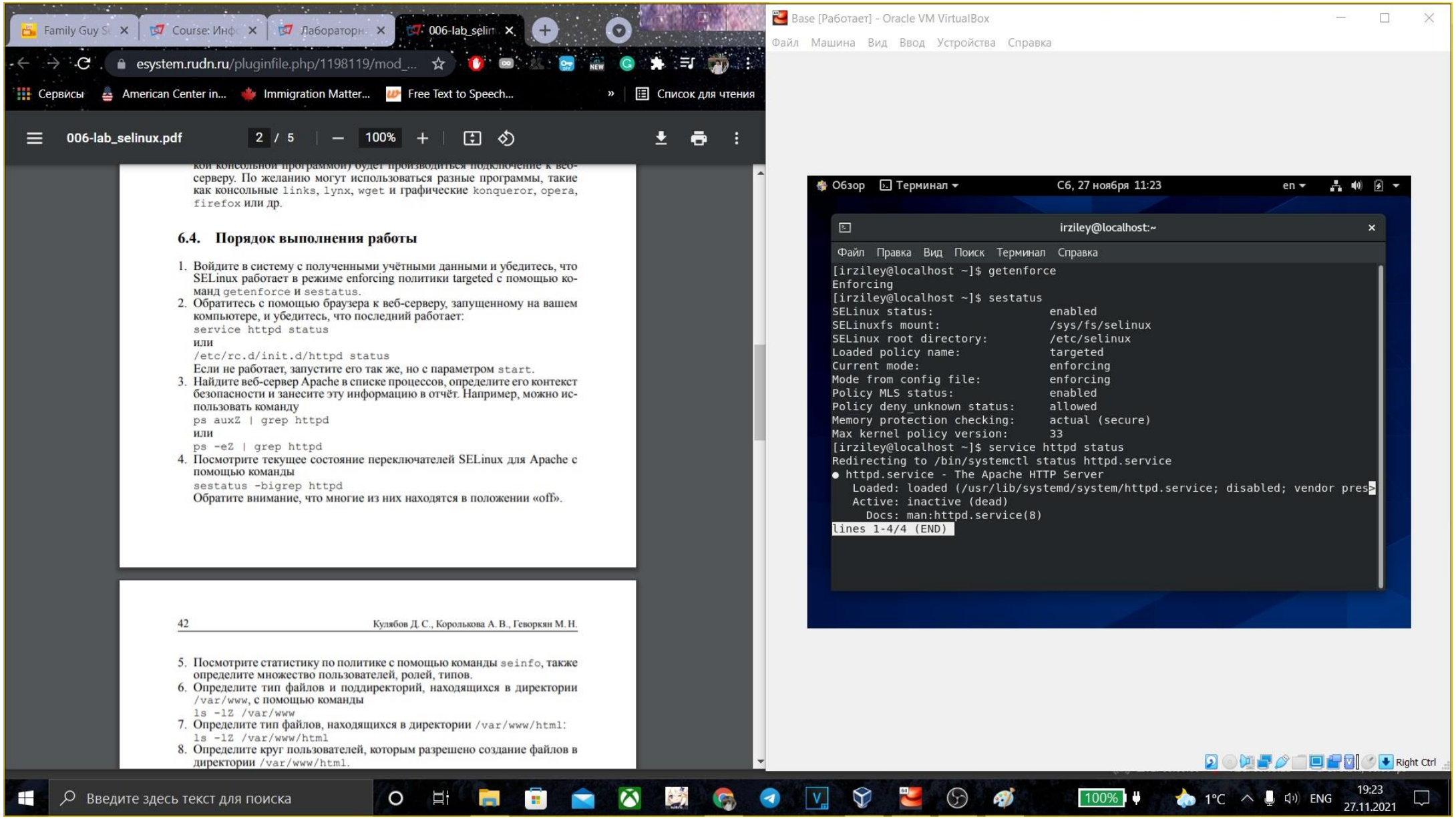
- Выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт.

Ход работы

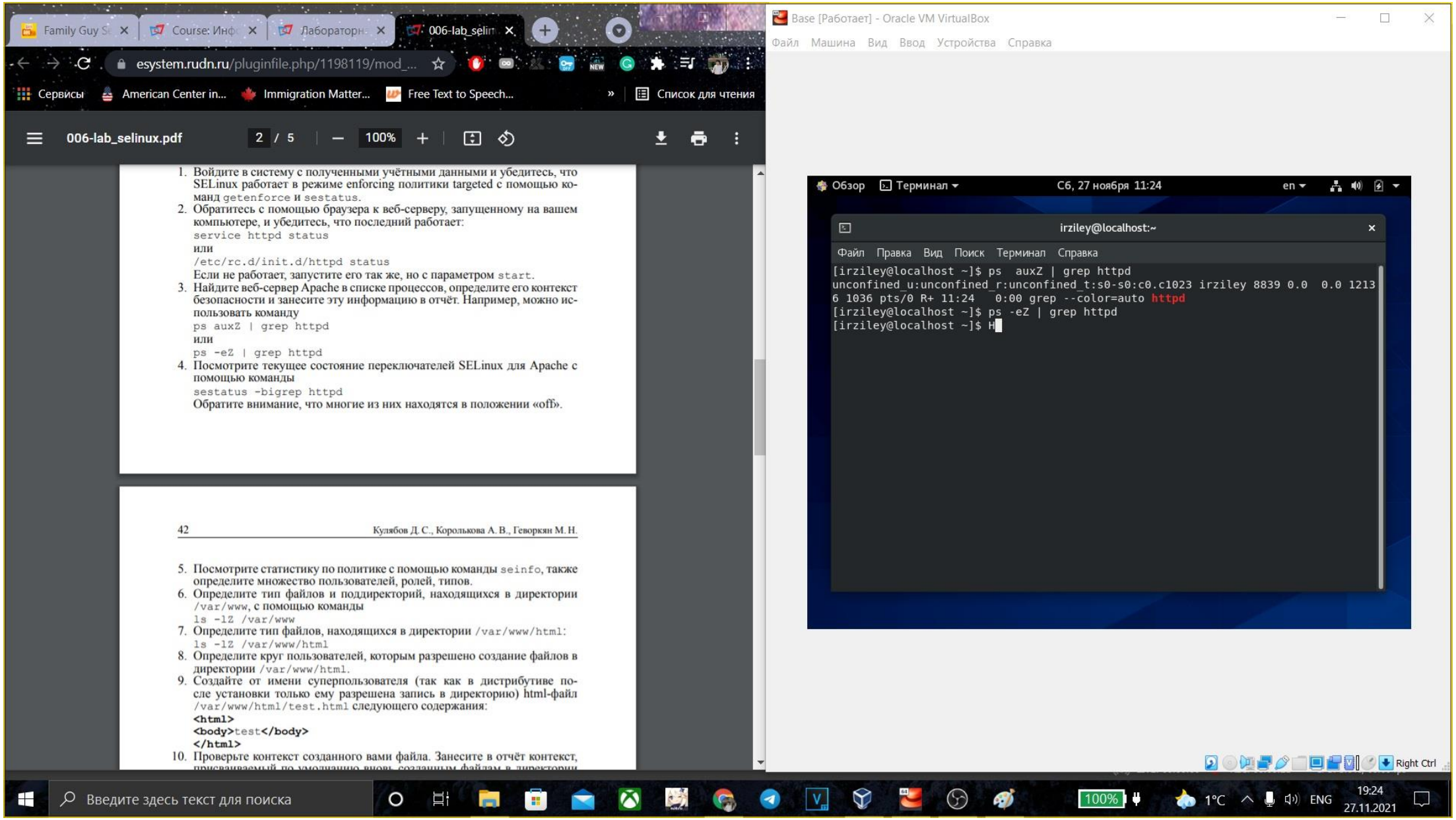
- 1.


esystem.rudn.ru/pluginfile.php/1198119/mod_...
Сервисы
American Center in...
Immigration Matter...
Free Text to Speech...
Список для чтения
006-lab_selinux.pdf
2 / 5
100%
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.
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Терминал
Сб, 27 ноября 11:20
en
irzileyelocalhost:~
Файл Правка Вид Поиск Терминал Справка
[irzileyelocalhost ~]$ setenforce
usage: setenforce [Enforcing | Permissive | 1 | 0]
[irzileyelocalhost ~]$ getenforce
Enforcing
[irzileyelocalhost ~]$ setstatus
bash: setstatus: команда не найдена...
[irzileyelocalhost ~]$ 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
[irzileyelocalhost ~]$
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:20
27.11.2021

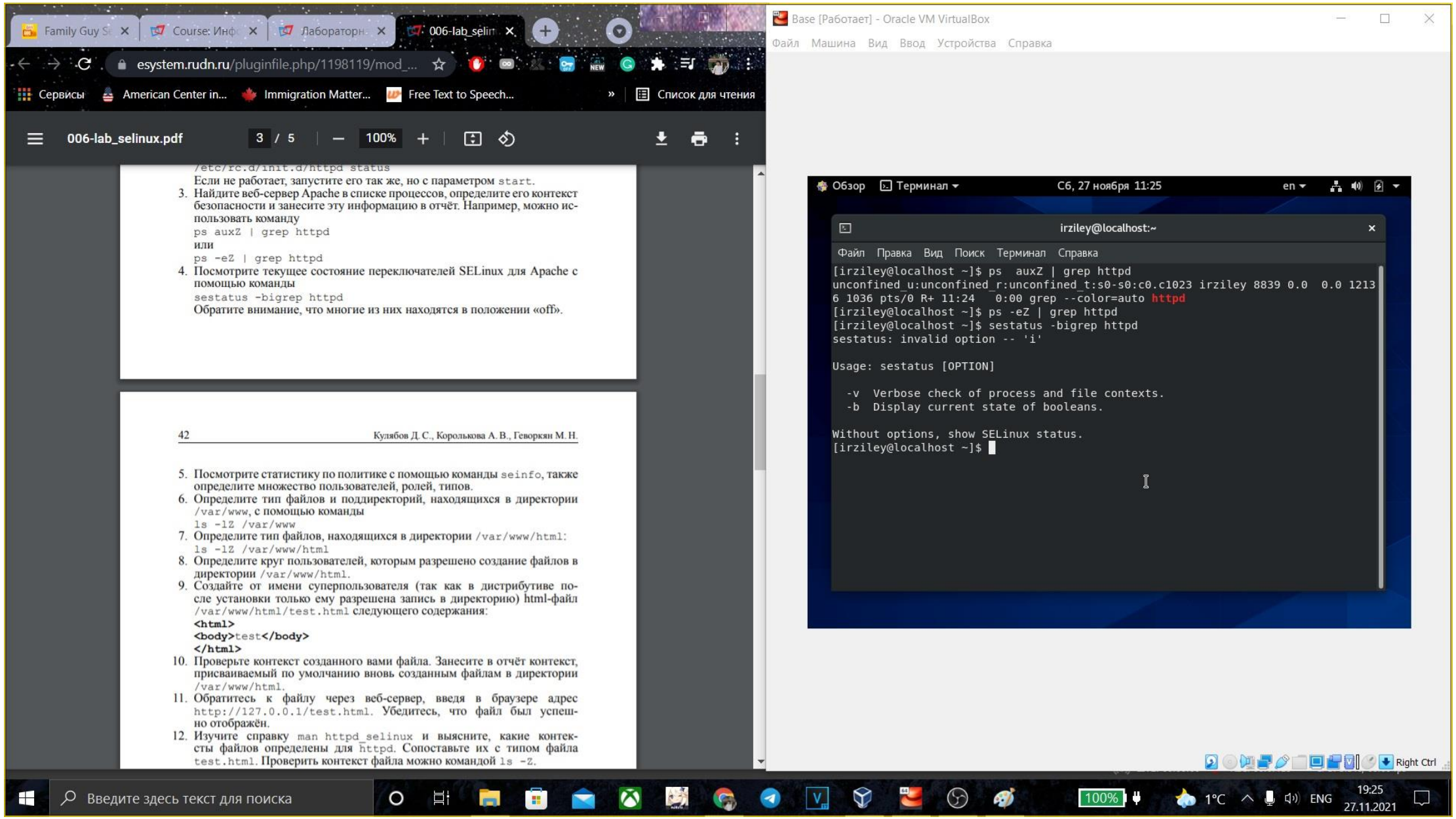
2.


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
2 / 5
100%
кой консольной 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.
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Терминал
Сб, 27 ноября 11:23
en
irziley@localhost:~
Файл Правка Вид Поиск Терминал Справка
[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 pres
Active: inactive (dead)
Docs: man:httpd.service(8)
lines 1-4/4 (END)
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:23
27.11.2021

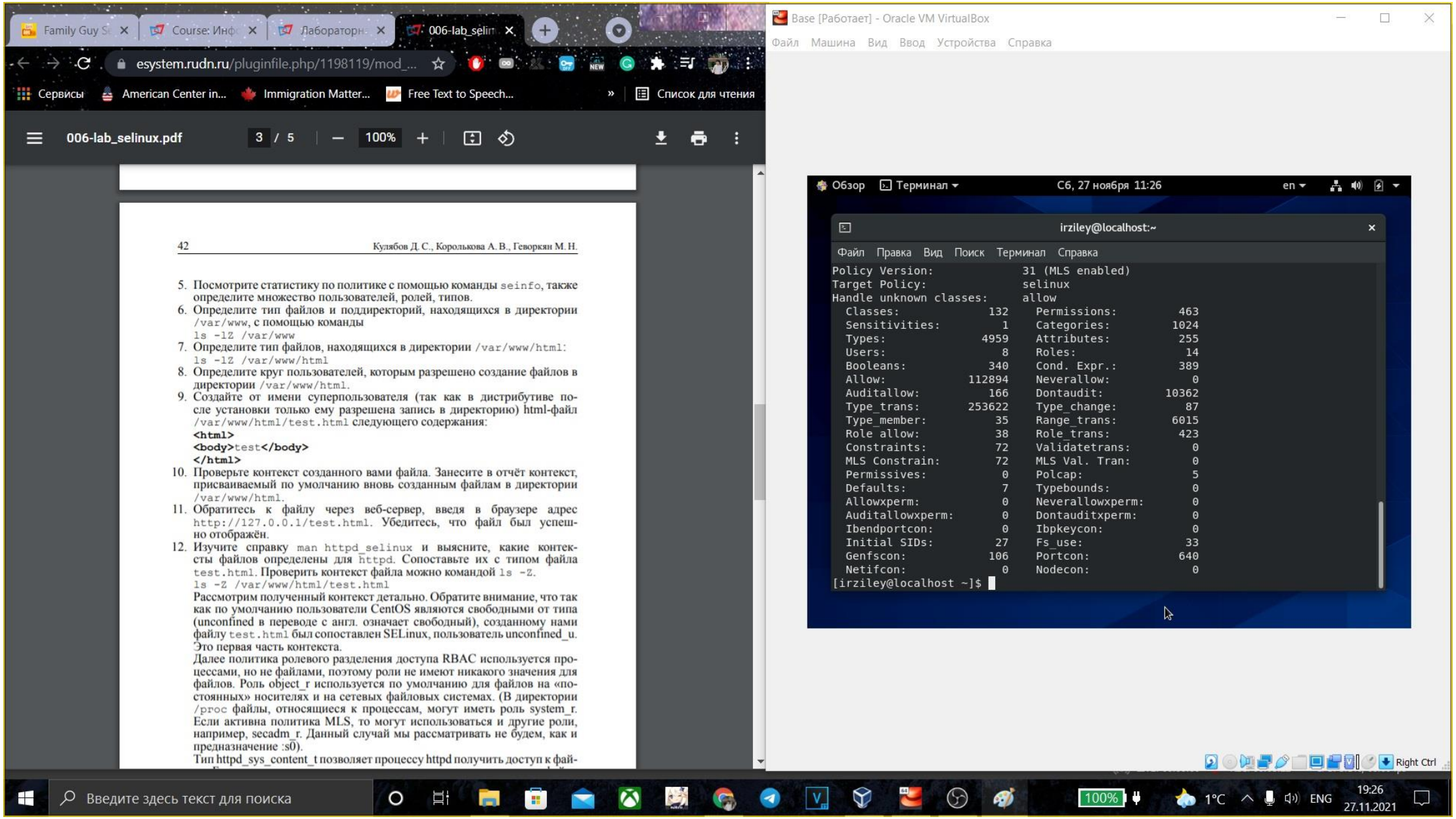
3.


Family Guy S
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
2 / 5
100%
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.
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,
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Терминал
Сб, 27 ноября 11:24
en
irziley@localhost:~
Файл Правка Вид Поиск Терминал Справка
[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
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:24
27.11.2021

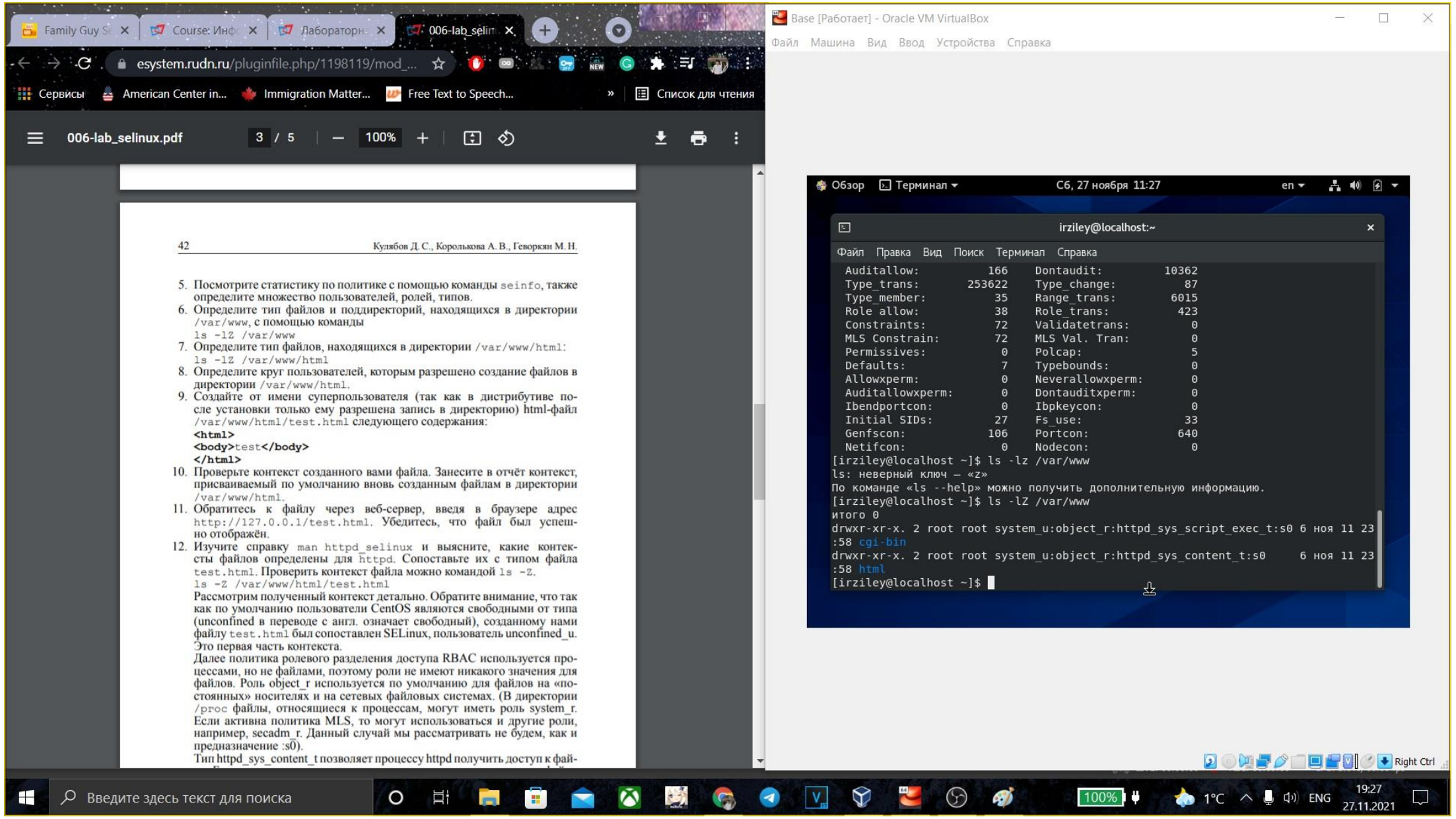
4.


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%
/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.
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.
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Терминал
Сб, 27 ноября 11:25
en
irziley@localhost:~
Файл Правка Вид Поиск Терминал Справка
[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 ~]$
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:25
27.11.2021

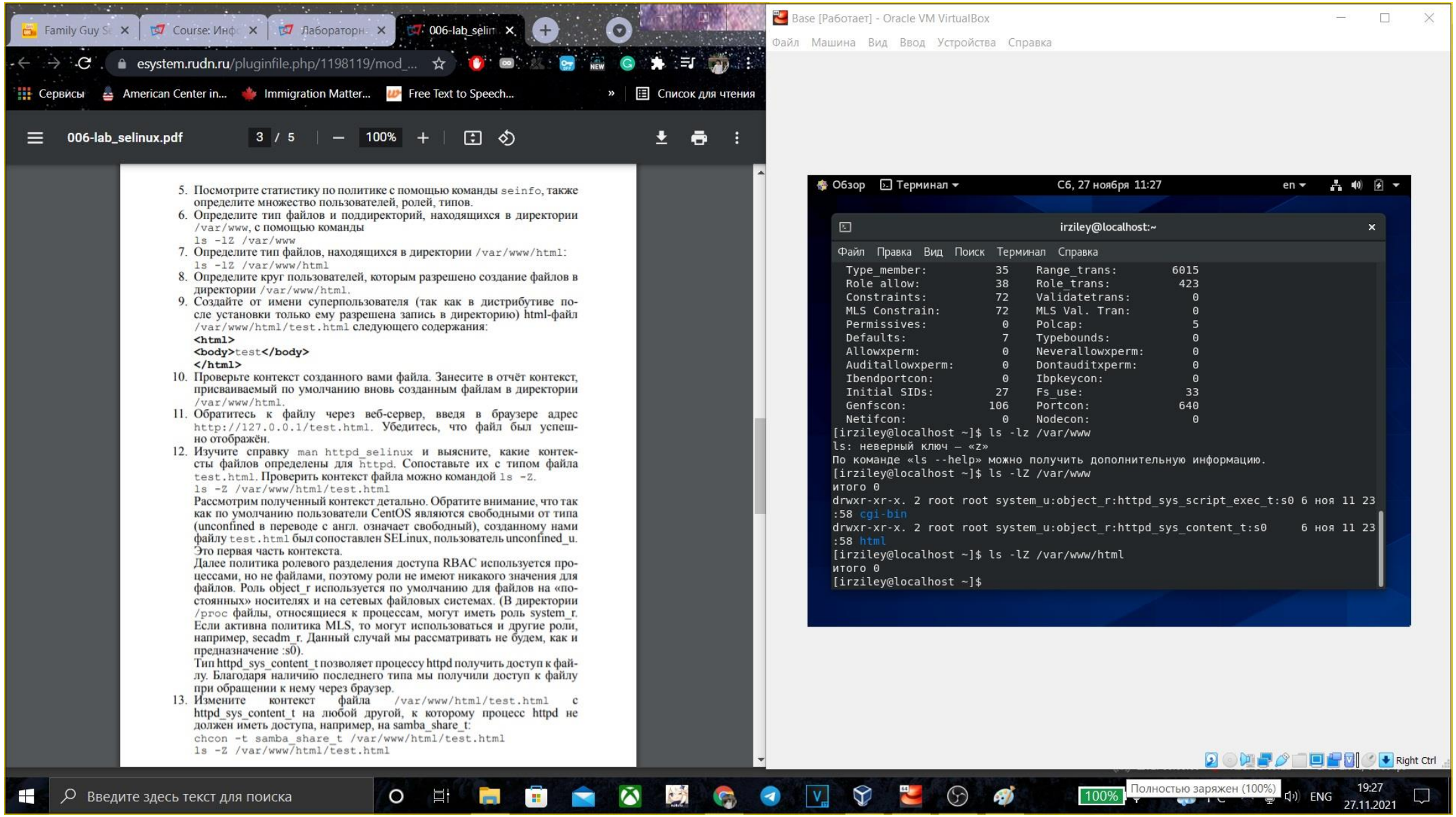
5.


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.
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.
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
Сб, 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 ~]$
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:26
27.11.2021

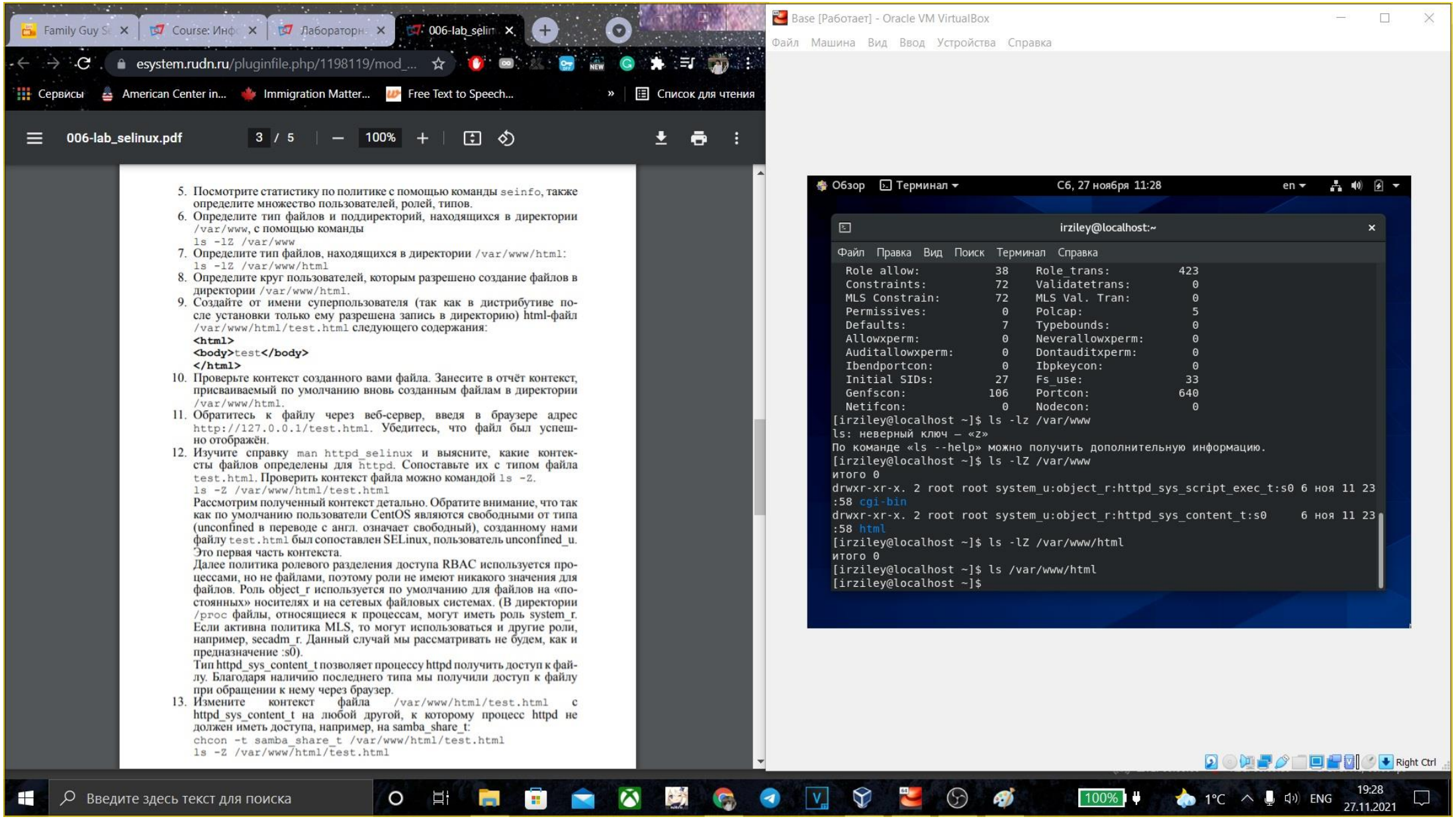
6.


Family Guy S
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.
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.
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
Сб, 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 ~]$
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:27
27.11.2021

7.


Family Guy S
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%
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.
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
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Терминал
Сб, 27 ноября 11:27
en
irziley@localhost:~
Файл Правка Вид Поиск Терминал Справка
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 ~]$ ls -lZ /var/www/html
итого 0
[irziley@localhost ~]$
Right Ctrl
Введите здесь текст для поиска
100%
Полностью заряжен (100%)
ENG
19:27
27.11.2021

8.



Family Guy S | Course: Инф | Лаборатор | 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%

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`.
    `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`

Base [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор | Терминал | Сб, 27 ноября 11:28 | en

irziley@localhost:~

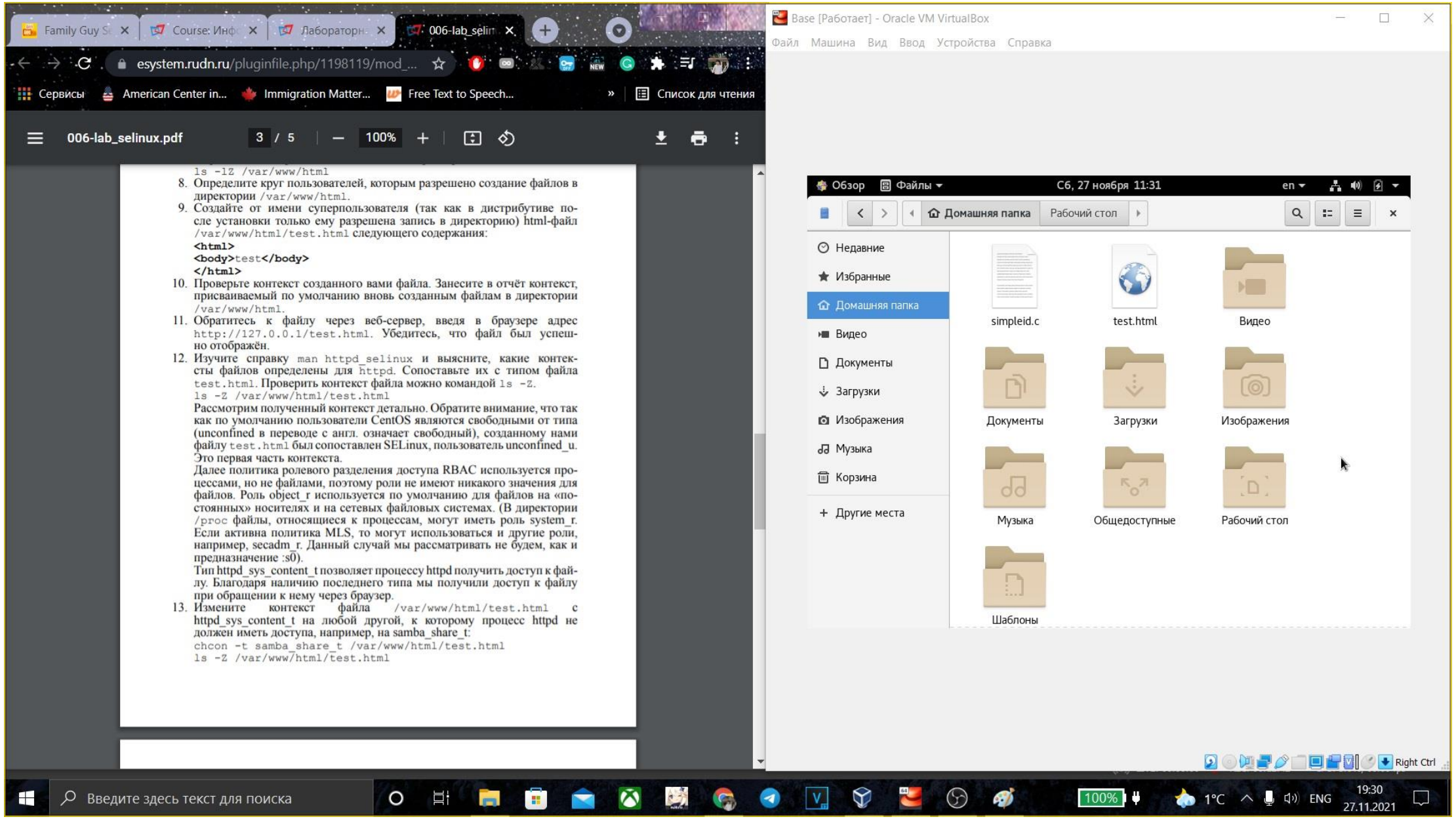
Файл Правка Вид Поиск Терминал Справка

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

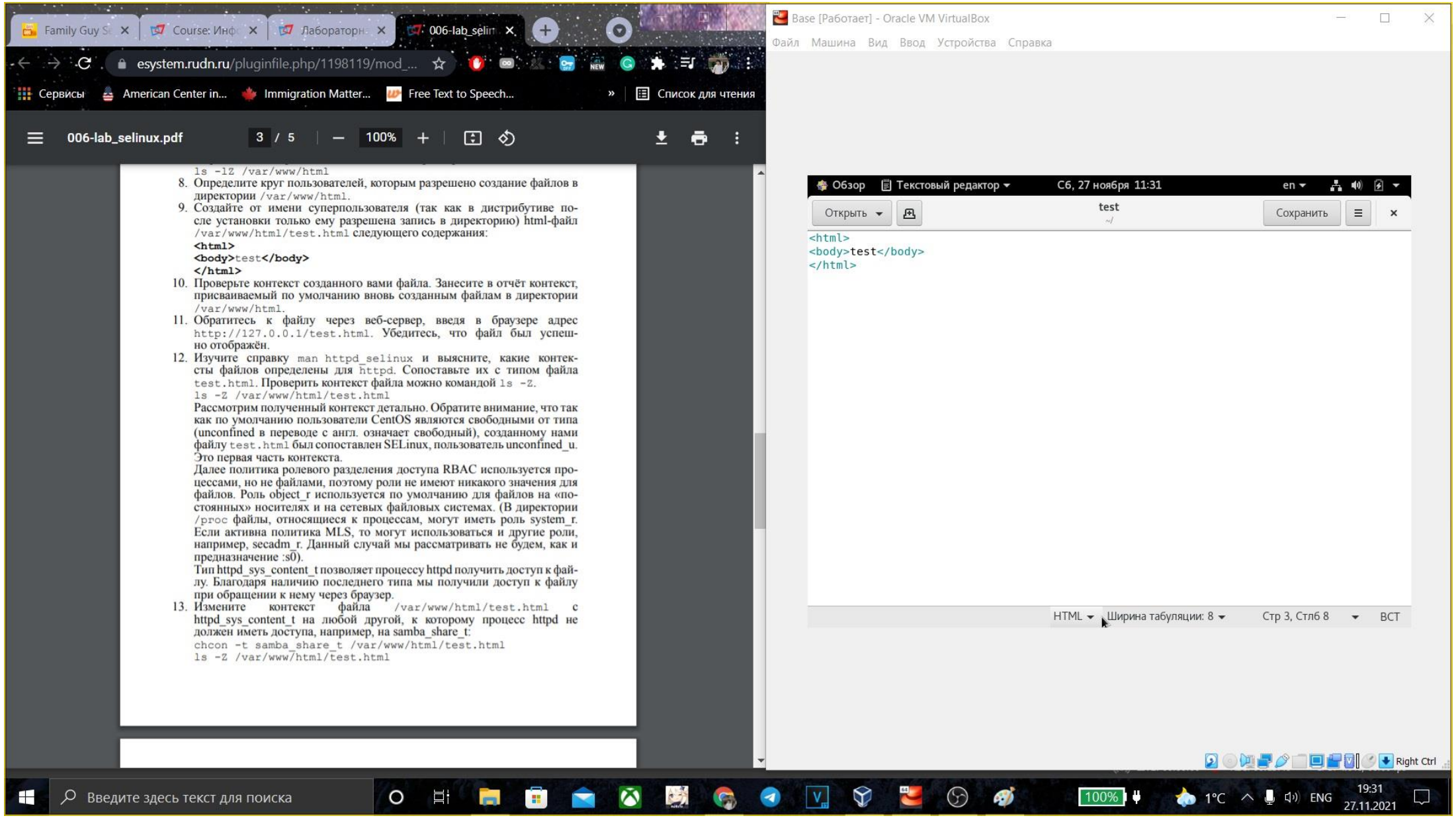
Right Ctrl

Введите здесь текст для поиска | 100% | 1°C | ENG | 19:28 27.11.2021

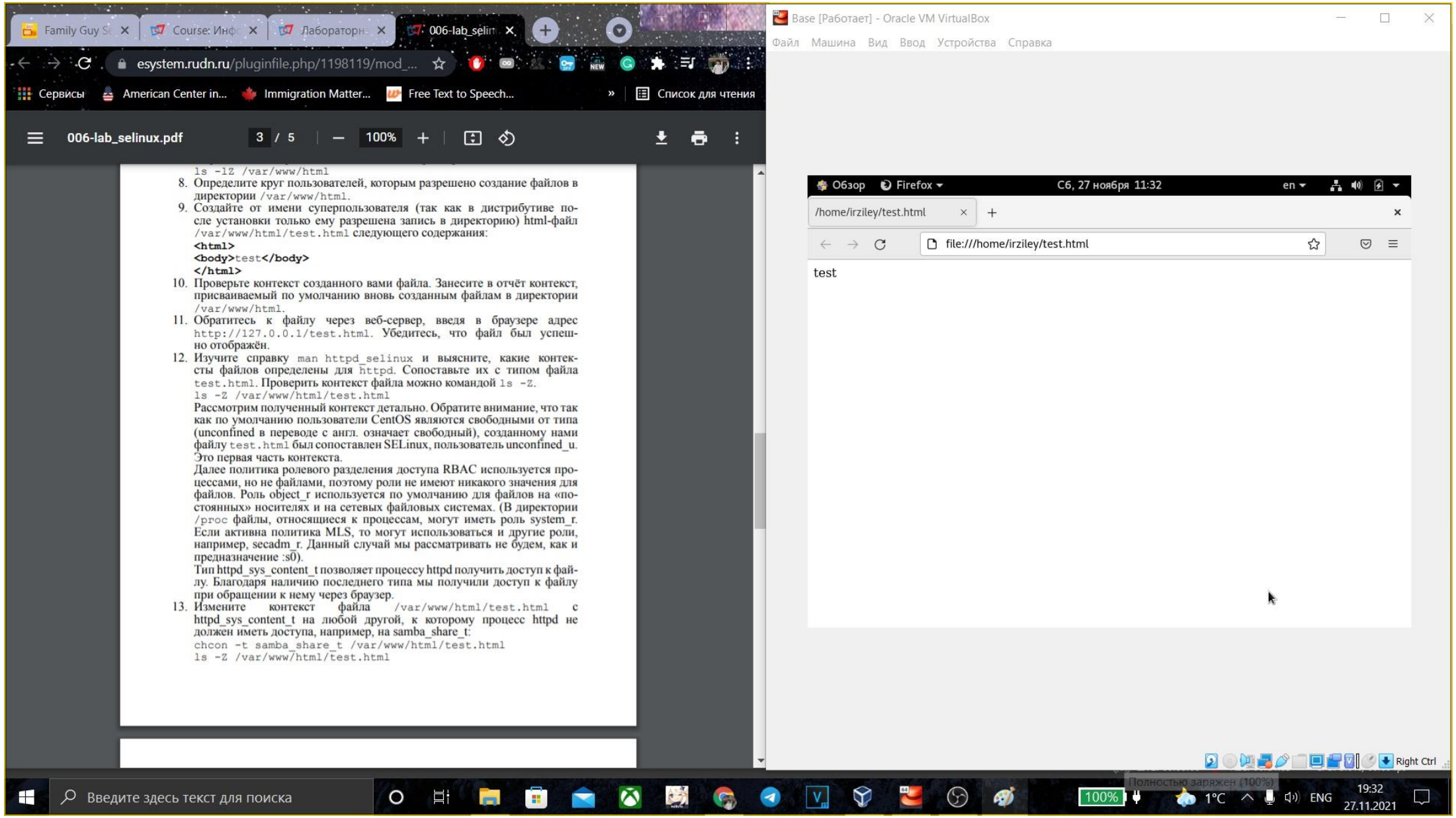
9.


Family Guy
Course: Инф
Лаборатор
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%
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.
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
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Файлы
Сб, 27 ноября 11:31
en
Домашняя папка
Рабочий стол
Недавние
Избранные
Домашняя папка
Видео
Документы
Загрузки
Изображения
Музыка
Корзина
Другие места
simpleid.c
test.html
Видео
Документы
Загрузки
Изображения
Музыка
Общедоступные
Рабочий стол
Шаблоны
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:30
27.11.2021

10.


Family Guy
Course: Инф
Лаборатор
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%
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.
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
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Текстовый редактор
Сб, 27 ноября 11:31
en
Открыть
test
~/
Сохранить
<html>
<body>test</body>
</html>
HTML
Ширина табуляции: 8
Стр 3, Стлб 8
ВСТ
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:31
27.11.2021

11.


Family Guy
Course: Инф
Лаборатор
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%
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.
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
Base [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор
Firefox
Сб, 27 ноября 11:32
en
/home/irziley/test.html
file:///home/irziley/test.html
test
Right Ctrl
Введите здесь текст для поиска
100%
1°C
ENG
19:32
27.11.2021

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.