Отчёт по лабораторной работе №6

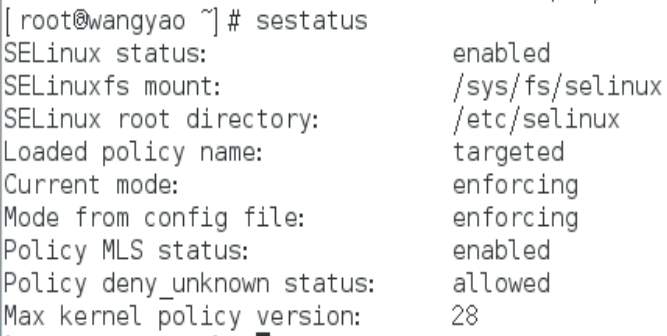
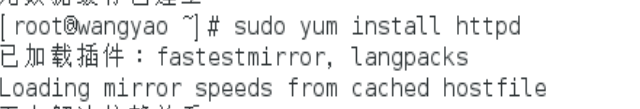
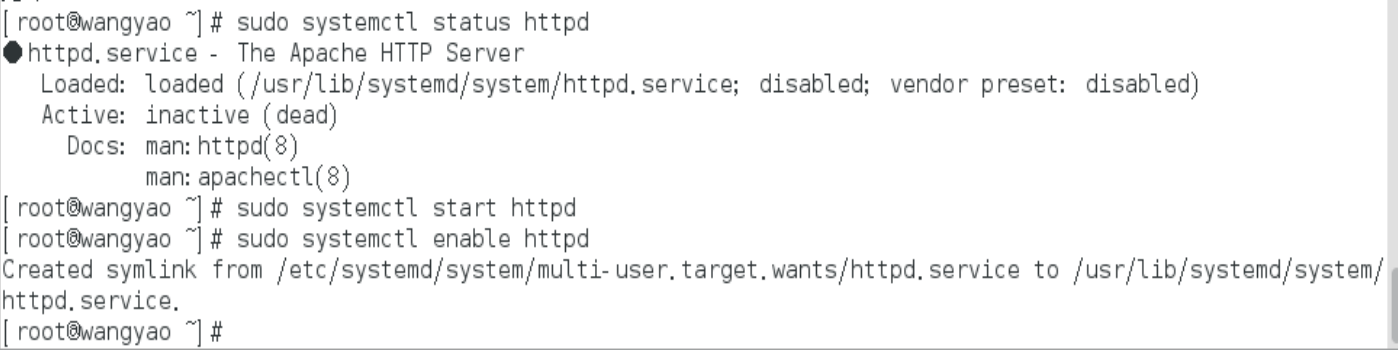
ван яо"

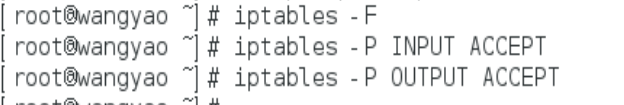
Содержание

# Цель работы

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

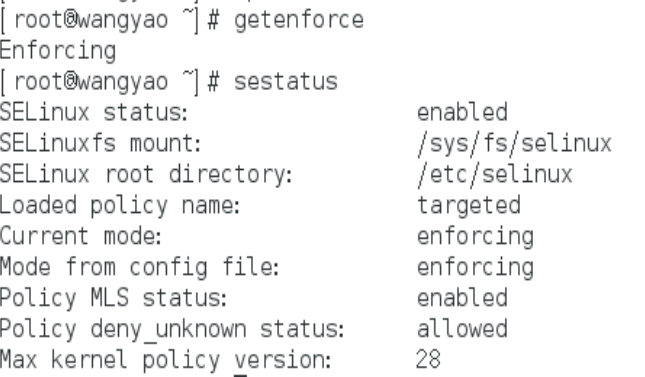
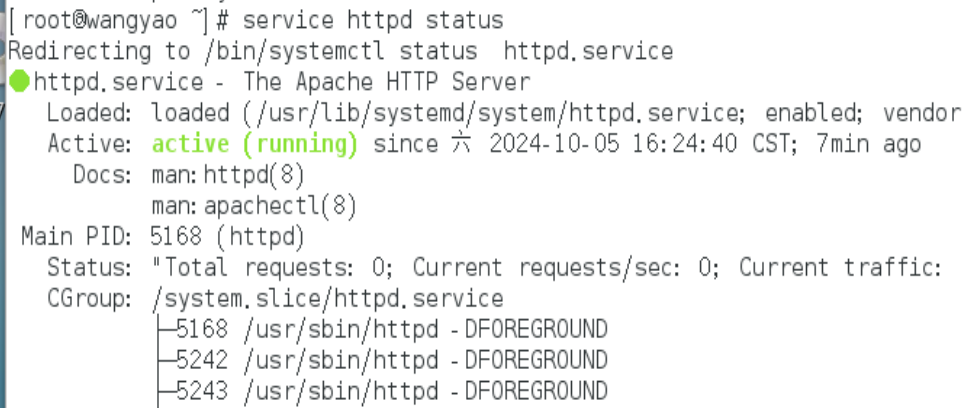
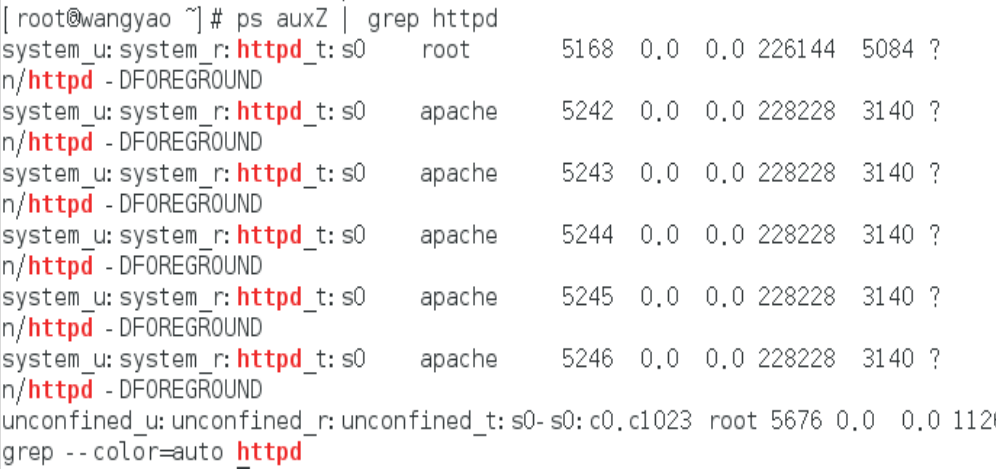
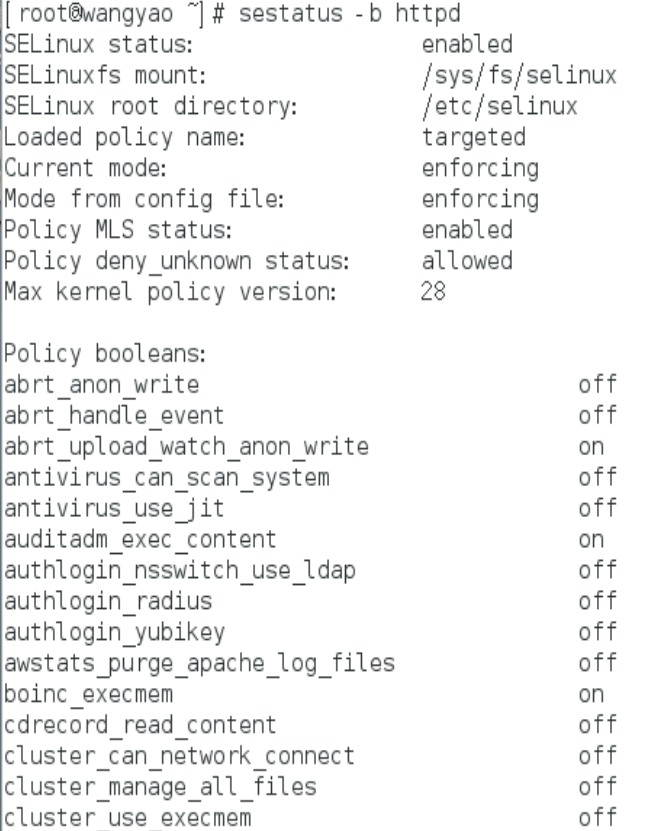
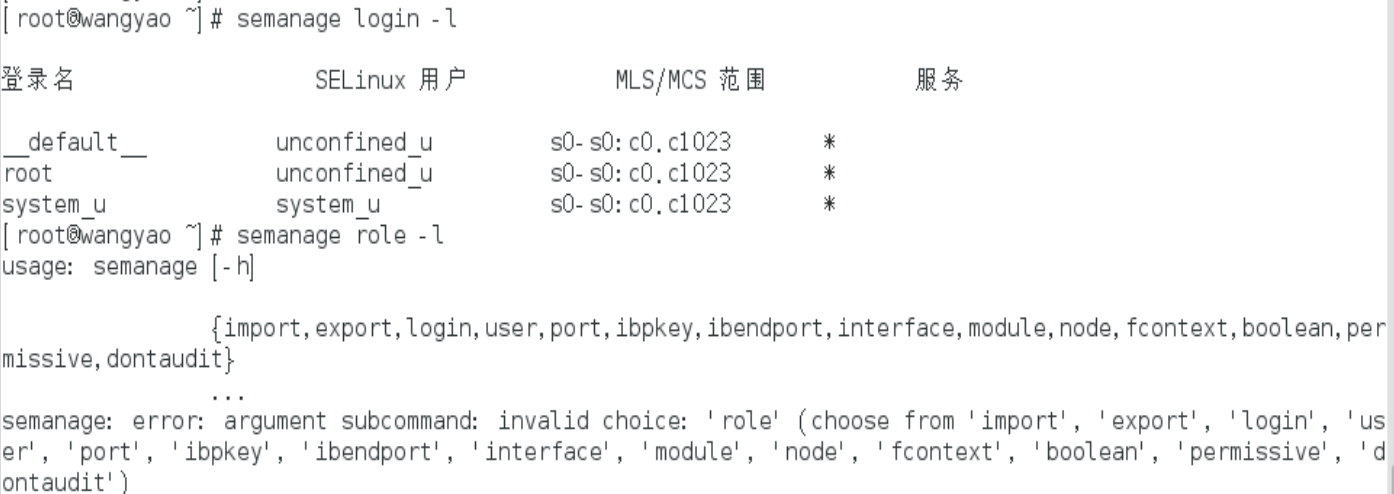
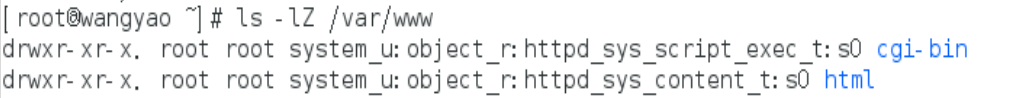
# Подготовка

1. При подготовке стенда обратите внимание, что необходимая для работы и указанная выше политика targeted и режим enforcing используются в данном дистрибутиве по умолчанию, т.е. каких-то специальных настроек не требуется. При этом следует убедиться, что политика и режим  
   включены, особенно когда работа будет проводиться повторно и велика  
   вероятность изменений при предыдущем использовании системы.  
     
     
   
2. При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл  
   */etc/selinux/config*, так и проверить используемый режим и  
   политику.
3. Необходимо, чтобы был установлен веб-сервер Apache. При установке  
   системы в конфигурации «рабочая станция» указанный пакет не ставится.
4. В конфигурационном файле \*/etc/httpd/httpd.conf \*необходимо задать параметр ServerName:  
   *ServerName test.ru*  
   чтобы при запуске веб-сервера не выдавались лишние сообщения об  
   ошибках, не относящихся к лабораторной работе.  
   fig:
5. Также необходимо проследить, чтобы пакетный фильтр был отключён  
   или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у  
   портам протокола tcp.  
   Отключить фильтр можно командами

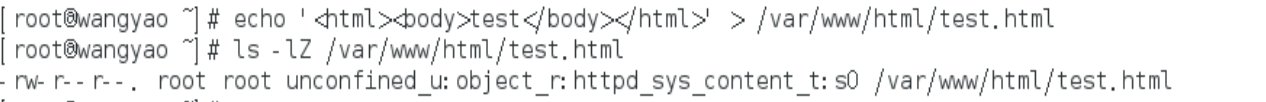
* iptables -F  
   iptables -P   
  INPUT ACCEPT iptables -P OUTPUT ACCEPT  
  либо добавить разрешающие правила:  
   iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
   iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
   iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
   iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT  
  

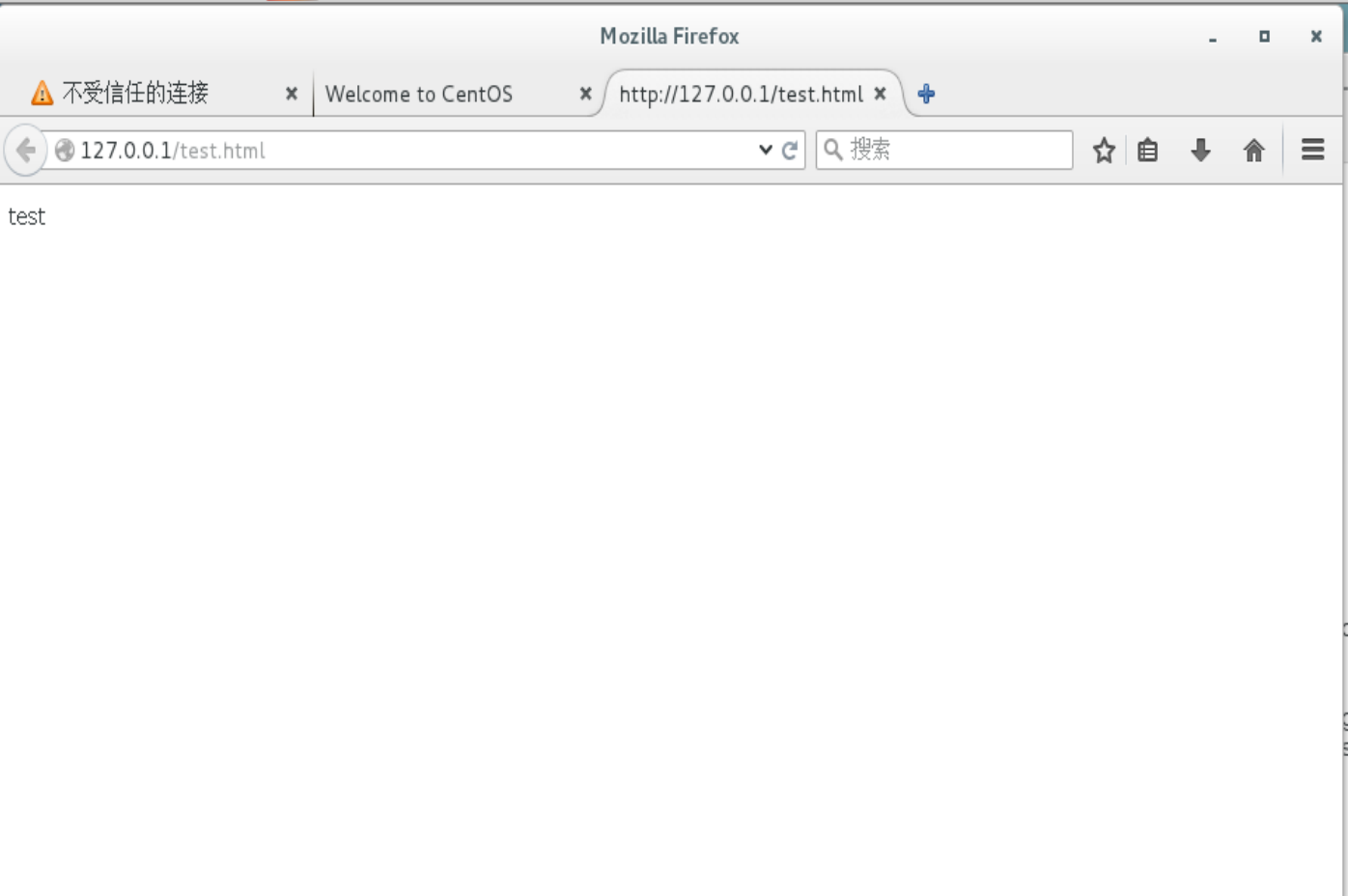
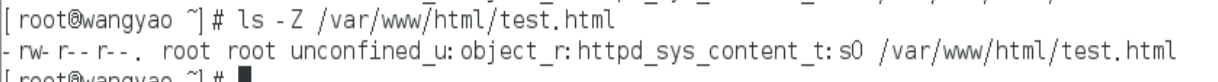
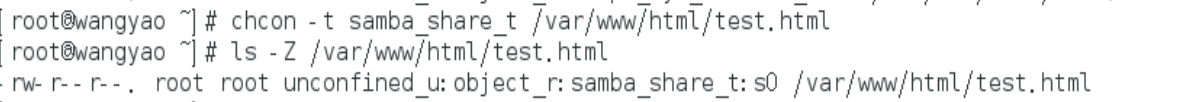
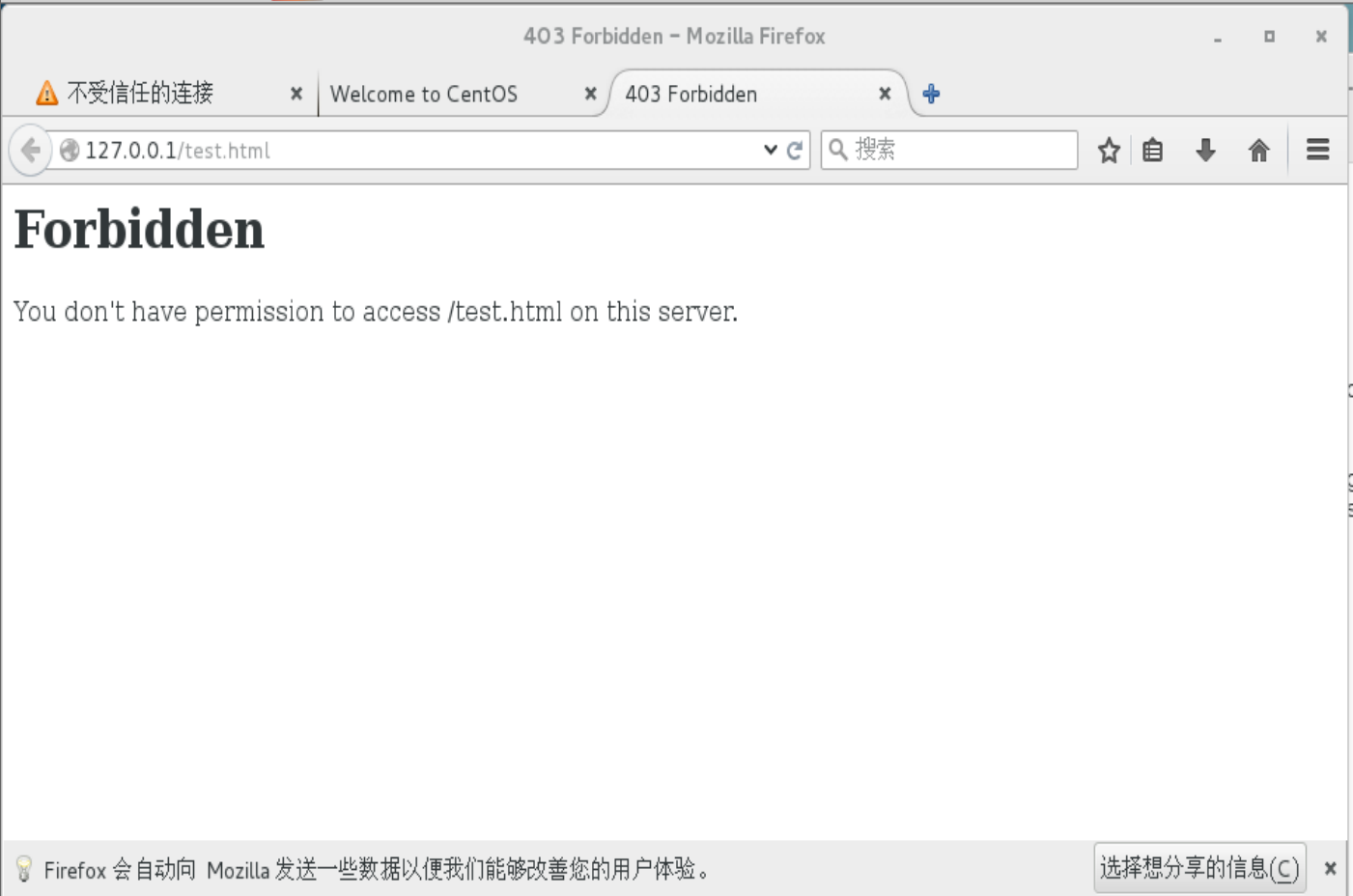
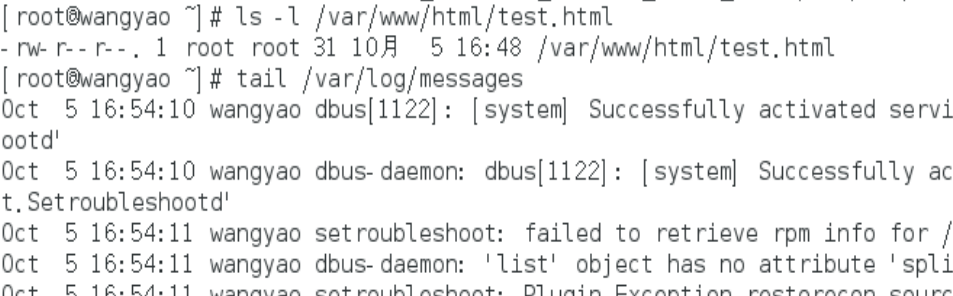
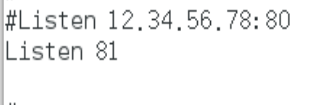
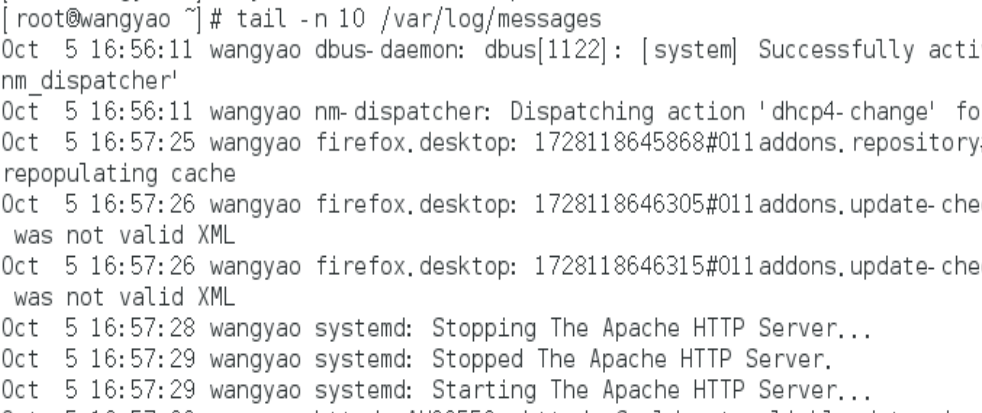
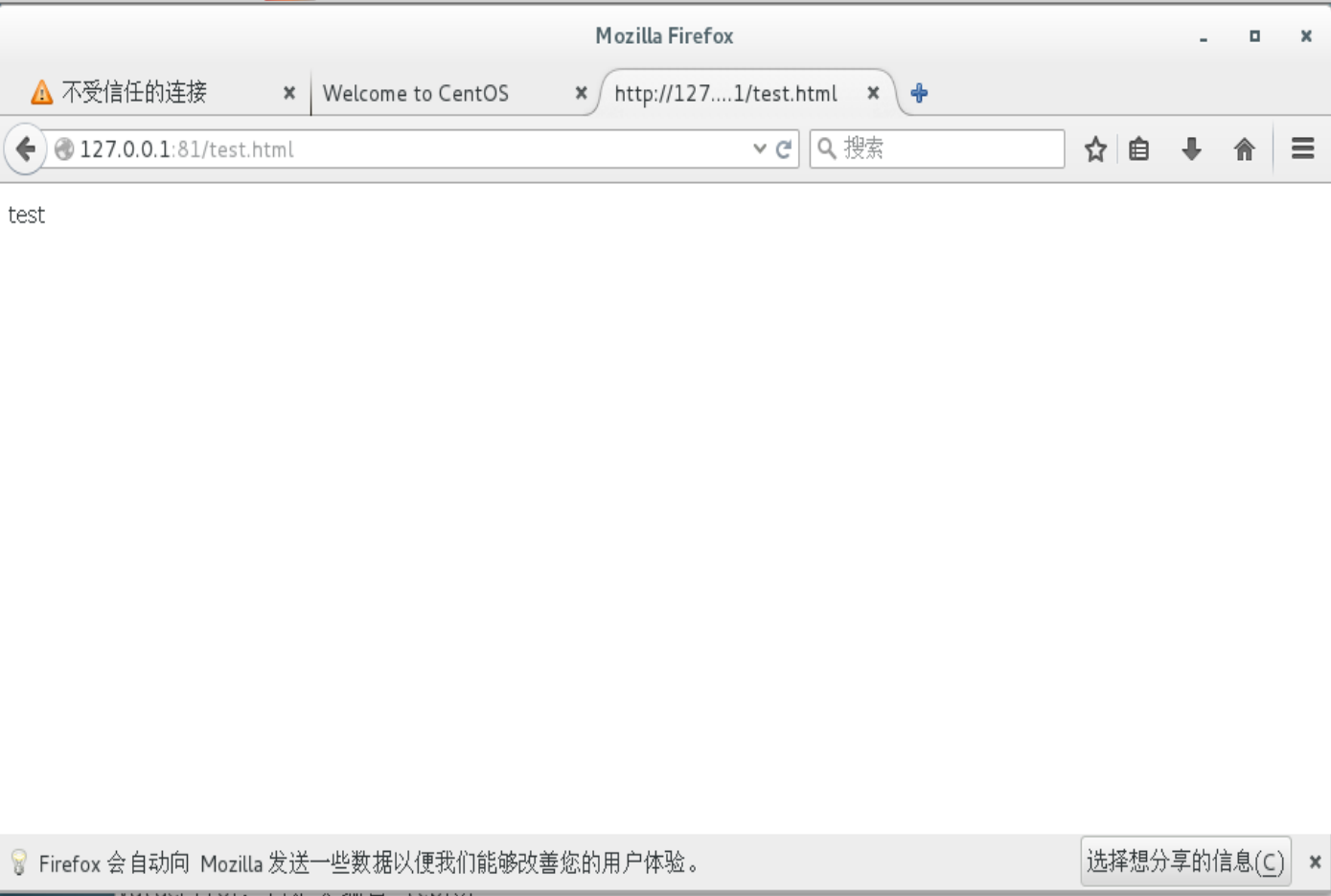
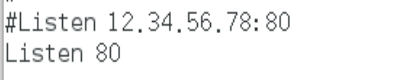
1. Обратите внимание, что данные правила не являются «точными» и рекомендуемыми на все случаи жизни, они лишь позволяют правильно организовать работу стенда.
2. В работе специально не делается акцент, каким браузером (или какой консольной программой) будет производиться подключение к вебсерверу. По желанию могут использоваться разные программы, такие  
   как консольные *links, lynx, wget* и графические *konqueror, opera,*  
   *firefox или др.*

# процесс выполнения задания

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».  
   
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  
   fig:
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:

* test



1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст,  
   присваиваемый по умолчанию вновь созданным файлам в директории  
   /var/www/html.
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес  
   <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён.  
   
3. 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  
   /ргос 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.  
   
4. 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  
   После этого проверьте, что контекст поменялся.  
   
5. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в  
   браузере адрес <http://127.0.0.1/test.html>. Вы должны получить  
   сообщение об ошибке:  
   Forbidden  
   You don't have permission to access /test.html on this server.  
   
6. Проанализируйте ситуацию. Почему файл не был отображён, если права  
   доступа позволяют читать этот файл любому пользователю?  
   ls -l /var/www/html/test.html  
   Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл:  
   tail /var/log/messages  
   Если в системе окажутся запущенными процессы setroubleshootd и  
   audtd, то вы также сможете увидеть ошибки, аналогичные указанным  
   выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно.  
   
7. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта  
   81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для  
   этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и  
   замените её на Listen 81.  
   
8. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните  
   почему?  
   **Перезапуск Apache (systemctl restart httpd) необходим для того, чтобы новые настройки вступили в силу и были применены корректно. Это гарантирует стабильную работу сервиса и помогает избежать возможных конфликтов и ошибок.**  
   fig:
9. Проанализируйте лог-файлы:  
   tail -nl /var/log/messages  
   Просмотрите файлы /var/log/http/error\_log,  
   /var/log/http/access\_log и /var/log/audit/audit.log и  
   выясните, в каких файлах появились записи.  
   
10. Выполните команду  
    semanage port -a -t http\_port\_t -р tcp 81  
    После этого проверьте список портов командой  
    semanage port -l | grep http\_port\_t  
    Убедитесь, что порт 81 появился в списке.  
    fig:
11. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему  
    он сейчас запустился, а в предыдущем случае не смог?  
    **Номер порта изменен**
12. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html:  
    chcon -t httpd\_sys\_content\_t /var/www/html/test.html  
    После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1:81/test.html>.  
    Вы должны увидеть содержимое файла — слово «test».  
    
13. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
14. 
15. Удалите привязку http\_port\_t к 81 порту:  
    semanage port -d -t http\_port\_t -p tcp 81  
    и проверьте, что порт 81 удалён.  
    
16. Удалите файл /var/www/html/test.html:  
    rm /var/www/html/test.html  
    

# выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1