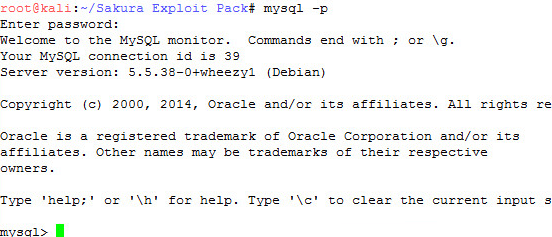
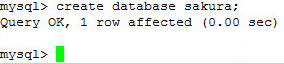
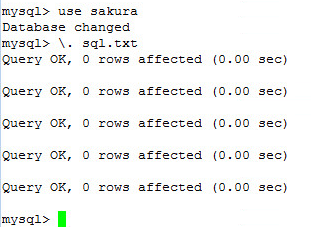
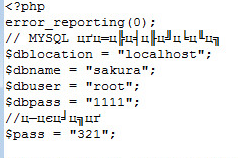
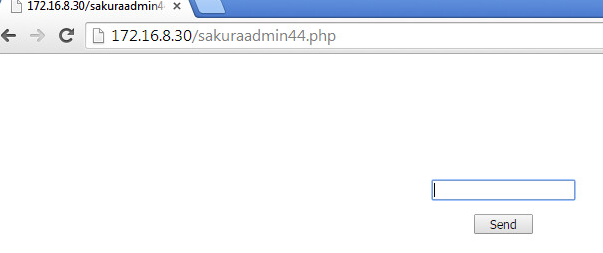
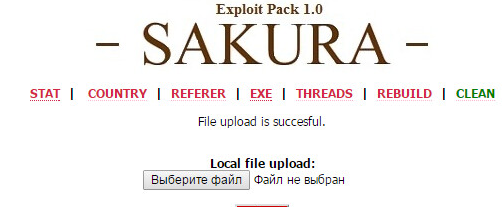
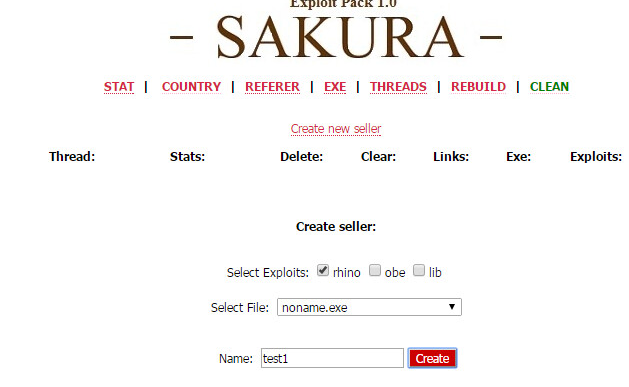
#### Часть 2. Изучение набора эксплойтов

В предыдущей части был рассмотрен механизм реализации атаки на клиентские компоненты с получением полного контроля над объектом атаки. После получения данного контроля можно, например, установить на этот узел произвольное программное обеспечение.

Такой вариант не очень удобен, если требуется выполнить атаку в отношении большого количества узлов. Для этой цели используются так называемые наборы эксплойтов. Далее в качестве примера рассматривается набор эксплойтов sakura.

Набор эксплойтов (exploit kit) будет установлен на машину Kali Linux.

1. Перейти в виртуальную машину Kali Linux
2. Скопировать программное обеспечение набора эксплойтов с указанного преподавателем сервера, например, в папку Sakura
3. Перейти в папку /root/Sakura
4. Подключиться к серверу mysql  
     
   
5. Создать базу sakura  
     
   
6. Подключиться к базе sakura  
     
   
7. Создать необходимые объекты (таблицы)  
     
   
8. Завершить работу с сервером mysql
9. Создать в каталоге /var/www папку sakura
10. Скопировать содержимое каталога sakura в папку /var/www/sakura  
      
    cp \* /var/www/sakura -R
11. Перейти в каталог /var/www/sakura
12. Отредактировать файл config.php, вписав туда параметры базы и сменив пароль для подключения (в данном случае 321)  
      
    
13. С виртуальной машины windows 7 подключиться к панели управления  
      
    
14. Ввести заданный ранее пароль, должна открыться панель управления
15. Перейти по ссылке ЕХЕ, далее нажать «Add file»
16. Загрузить произвольный файл  
      
    На практике здесь должен быть загружен файл, который должен запускаться на компьютере пользователя при срабатывании эксплойта, например, рассмотренный ранее «бот».  
      
    
17. Далее перейти по ссылке THREADS и нажать «Create new seller»
18. Выбрать загруженный ранее исполняемый файл (в данном случае – noname.exe), затем связать его с эксплойтом и нажать Create  
      
    
19. Созданная ссылка может быть использована для заражения компьютера пользователя (необходимо лишь заменить адрес сервера)
20. Перейти на компьютер User PC (cl1), затем перейти по созданной ссылке (в зависимости от версии программного обеспечения на компьютере пользователя может отработать экплойт)

Перейти по ссылке STAT, убедиться, что добавился один новый узел  
  
