Министерство образования Республики Беларусь

Учреждение образования

“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №5

«Идентификация уязвимостей сетевых приложений по косвенным признакам»

Выполнил:

Студент группы МС-42

Рыбалкин Д.С.

Проверил: Грищенко В.В.

2022

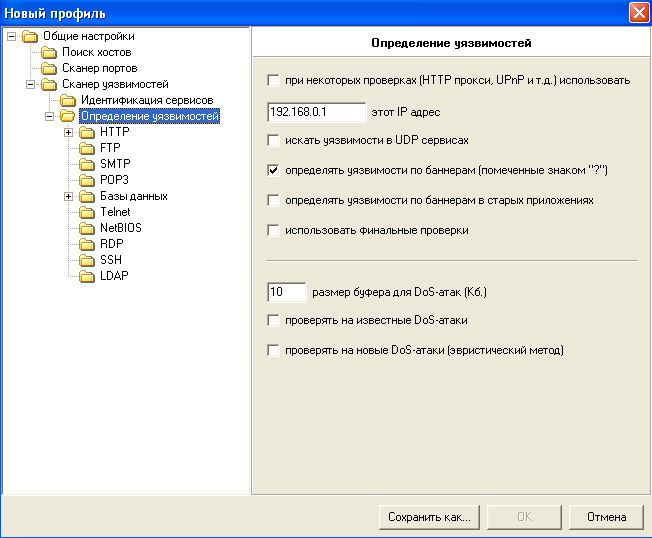
**Лабораторная работа №5**

***Цель работы:*** обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

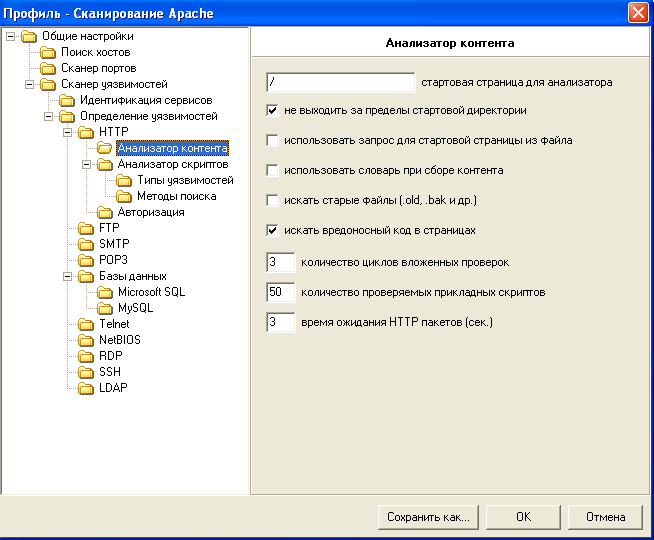
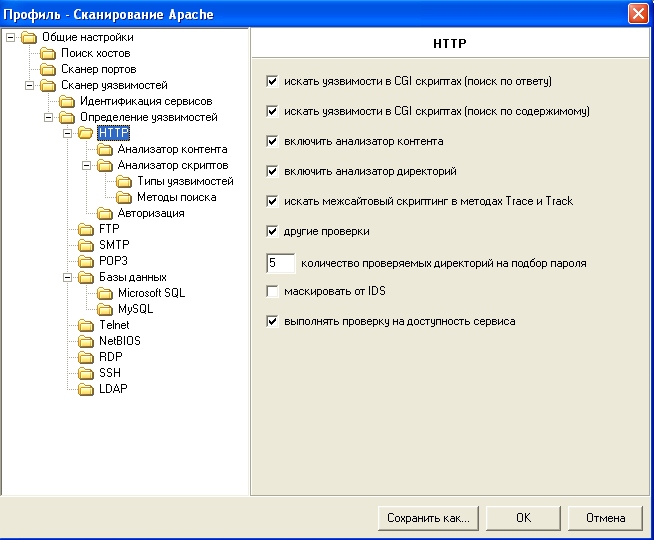
**Постановка задачи:** Выполнить идентификацию уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.

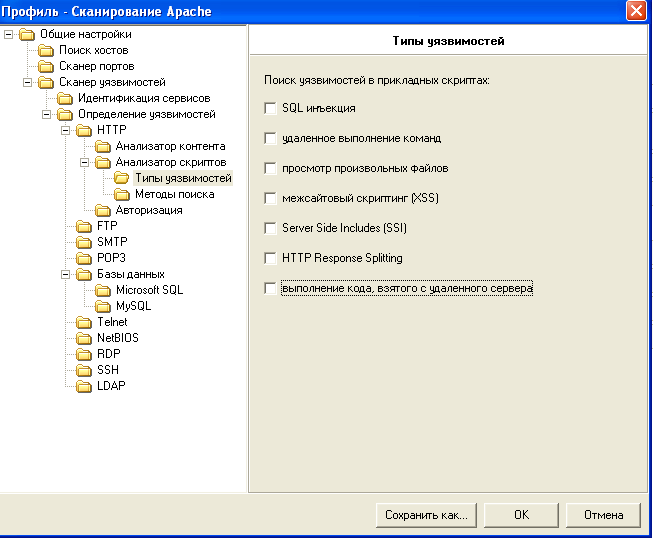
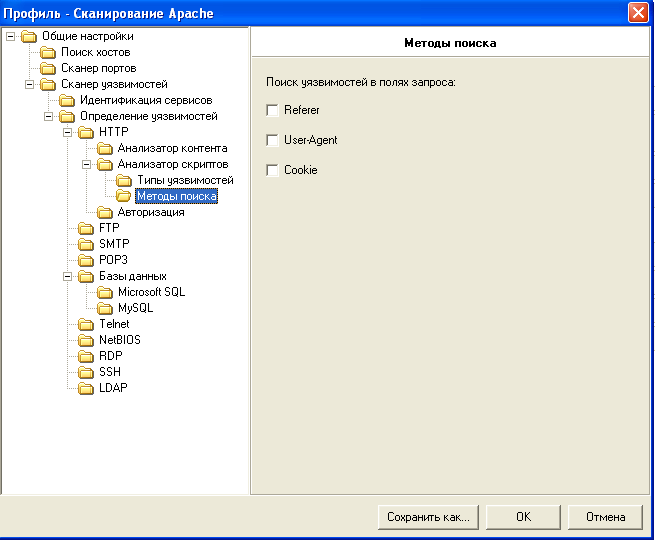
**Шаг 1.** Создать профиль сканирования «Сканирование Apache». Перечень сканируемых портов ограничить портом 80. Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoSатаки», «Проверять на новые DoS-атаки».





**Шаг 2.** В секции «НТТР» включить опцию «Включить анализатор директорий», остальные опции отключить. В секции «Анализатор контента» включить опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставить опцию «Искать уязвимости в GET запросах», отключить остальные опции. В секциях «Типы уязвимостей» и «Методы поиска» отключить все опции. В секции «Подбор учётных записей» отключить опцию «Подбирать учётные записи». Сохранить профиль.

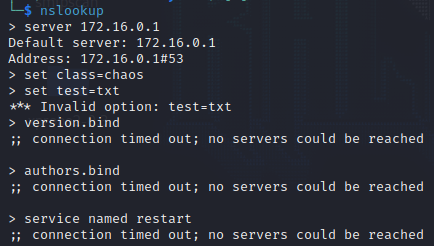


**Шаг 3.** Создать копию профиля «Сканирование Apache», задать ему имя «Сканирование сетевых служб». Перечень сканируемых портов ограничить портами 22 и 53. В секции «Сканер UDPсервисов» отключить все опции, кроме DNS. Сменить профиль для задачи «Сканирование Linux».



**Шаг 4.** Проанализировать результаты сканирования службы DNS, обратить внимание на версию BIND. Выполнить ручную проверку наличия уязвимостей, использую средство nslookup:



**Вывод:** в ходе лабораторной работы были изучены методы и средства идентификации уязвимостей по косвенным признакам в сетевых приложениях КС, выполнена идентификация уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.