Гомельский Государственный Университет им. Ф. Скорины

**Отчёт по лабораторной работе**

**«Идентификация уязвимостей сетевых приложений по косвенным признакам»**

**Проверил:**

Грищенко В.В.

**Студенка МС – 42:**

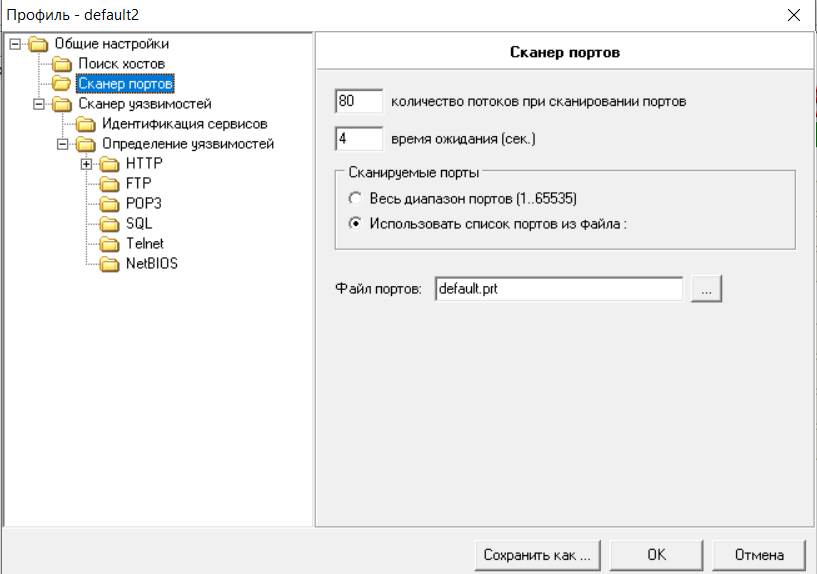
Кислова К.В.

Г. Гомель

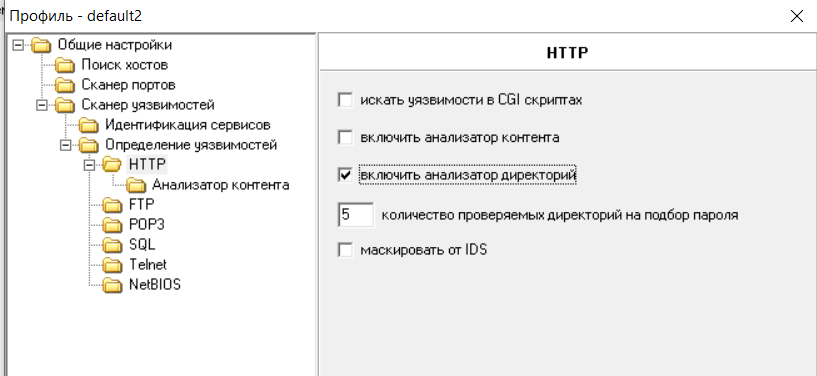
**Цель работы**

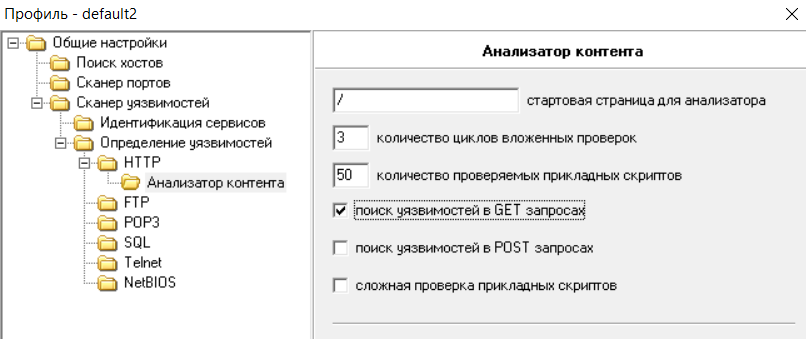
Обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

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»

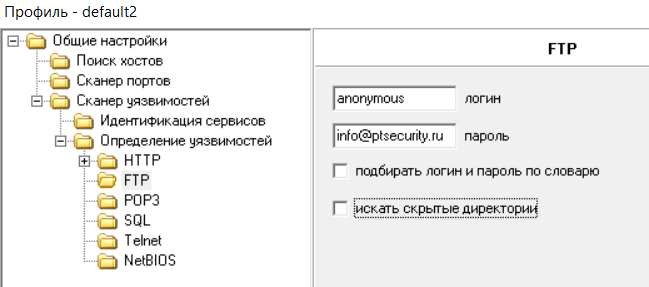


В секции «НТТР» включить опцию «Включить анализатор директорий», остальные опции отключить. В секции «Анализатор контента» включить опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставить опцию «Искать уязвимости в GET запросах», отключить остальные опции. В секциях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





Создать задачу «Сканирование Linux», добавить в нее узел S1. Запустить на сканирующем узле анализатор протоколов. Выполнить сканирование узла S1. Обратить внимание на уязвимости, найденные на порту 80 веб-сервера Apache, а также на результаты идентификации службы НТТР. Найти результаты работы анализатора каталогов. Проверить наличие найденных уязвимостей вручную. Просмотреть трассировку сканирования в анализаторе протоколов.



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

