Министерство образования Республики Беларусь

Учреждение образования

«Гомельский государственный университет

имени Франциска Скорины»

Отчёт по лабораторной работе №5

«Идентификация уязвимостей сетевых приложений по косвенным признакам»

Выполнил студент группы МС-42: Казак И.В.

Проверил:

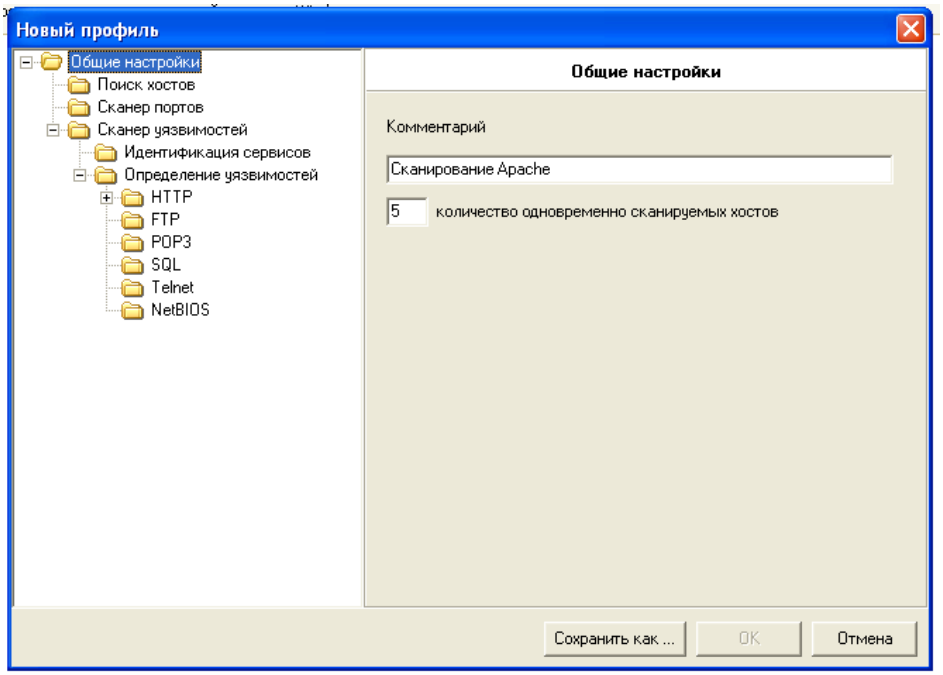
Старший преподаватель Грищенко В.В.

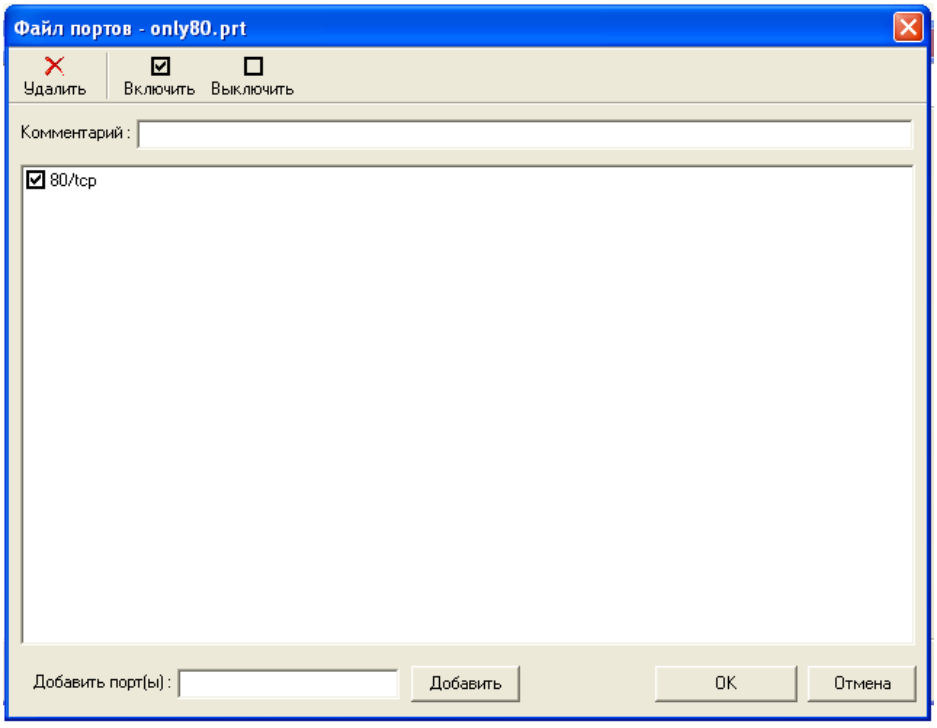
Гомель 2022

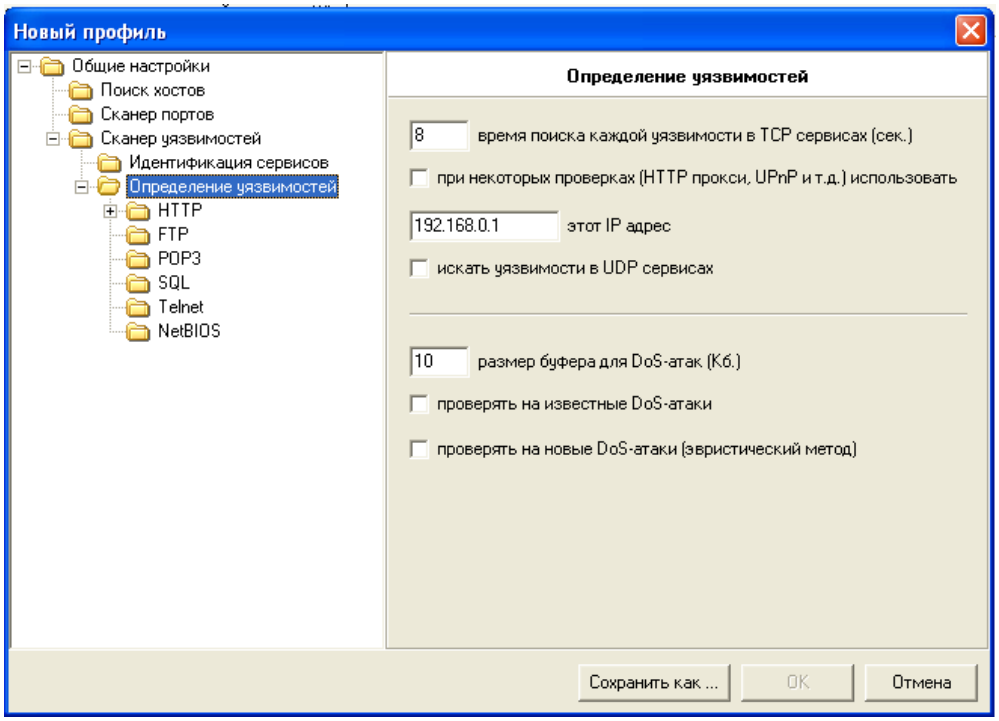
Цель работы: обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

Ход работы.

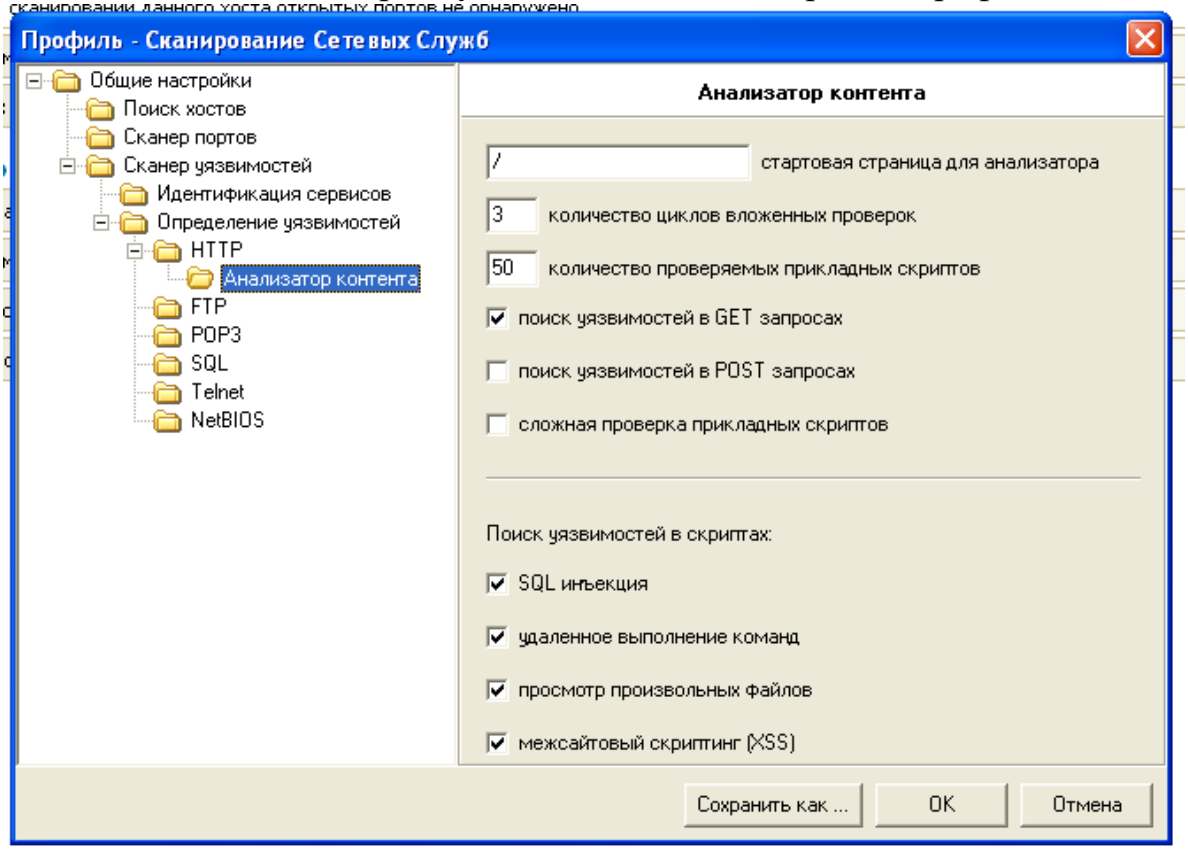
Шаг 1. Создадим профиль сканирования «Сканирование Apache». Перечень сканируемых портов ограничим портом 80. Отключим сканирование служб UDP, в секции «Определение уязвимостей» отключим опции «Использовать финальные проверки», «Проверять на известные DoSатаки», «Проверять на новые DoS-атаки».







Шаг 2. В секции «HTTP» включим опцию «Включить анализатор директорий», остальные опции отключим. В секции «Анализатор контента» включим опцию «Не выходить за пределы стартовой страницы». В секции «Анализатор сценариев» оставим опцию «Искать уязвимости в GET запросах», отключим остальные опции. В секциях «Типы уязвимостей» и «Методы поиска» отключим все опции. В секции «Подбор учётных записей» отключим опцию «Подбирать учётные записи». Сохраним профиль.



Шаг 3. Создадим копию профиля «Сканирование Apache», зададим ему имя «Сканирование сетевых служб». Перечень сканируемых портов ограничим портами 22 и 53. В секции «Сканер UDPсервисов» отключим все опции, кроме DNS. Сменим профиль для задачи «Сканирование Linux».


Хост
172.16.0.21

Информация

При сканировании данного хоста открытых портов не обнаружено.	
Время отклика:	< 1 мсек
TTL:	64

Параметры сканирования

Начало сканирования:	16:07:15 27.11.2022
Время сканирования:	00:00:07
Версия:	7.7 Build 3100
Профиль:	Сканирование Сетевых Служб.prf

Шаг 4. Проанализируем результаты сканирования службы DNS, обратим внимание на версию BIND. Выполним ручную проверку наличия уязвимостей, используя средство nslookup:

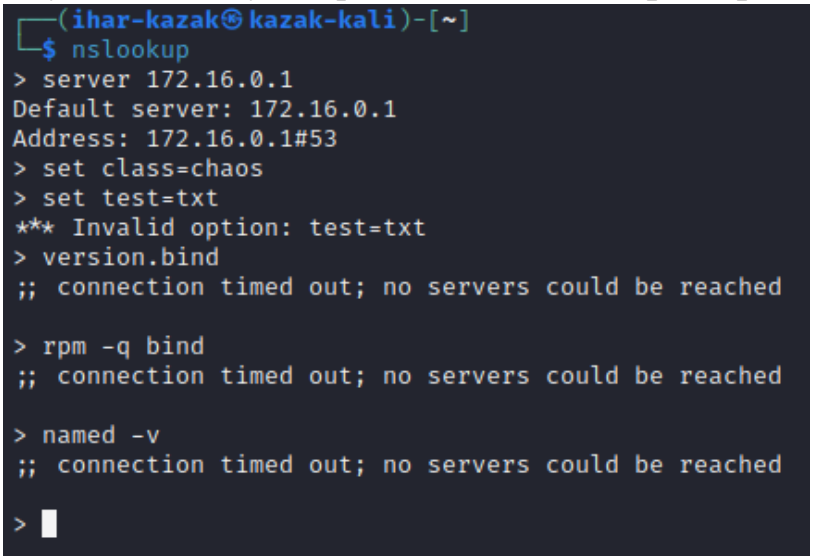
C:>nslookup
>server 192.168.56.102
>set class=chaos
>set test=txt
>version.bind

Выполнить запрос authors.bind:

>authors.bind

Проверим версию ПО bind, выполнив команду: **named -v**

Проверим установленную версию пакета bind: **rpm –q bind**



Вывод: в ходе лабораторной работы познакомились и воспользовались методами и средствами идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.