

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
Созинов Л.В.
Проверил:
Грищенко В.В.

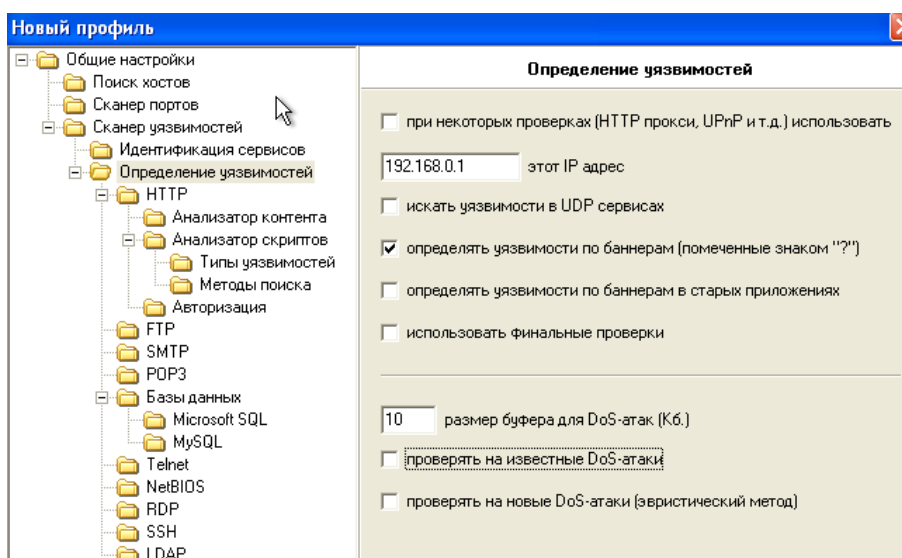
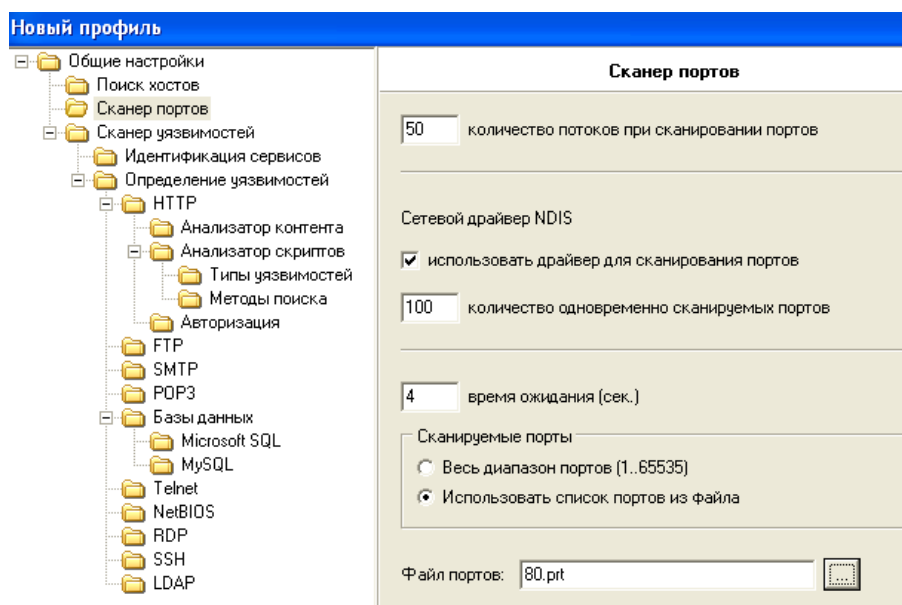
Лабораторная работа №5

Идентификация уязвимостей сетевых приложений по косвенным признакам

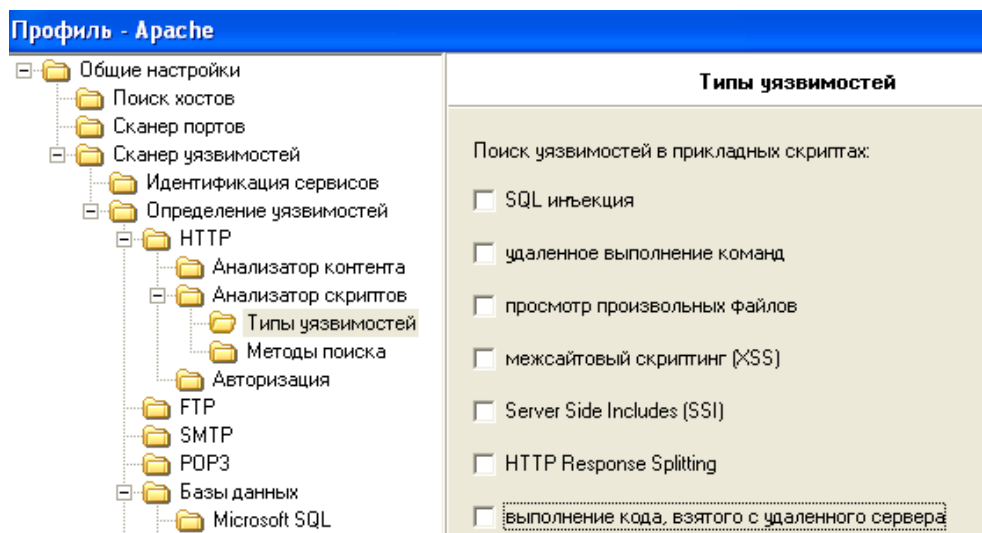
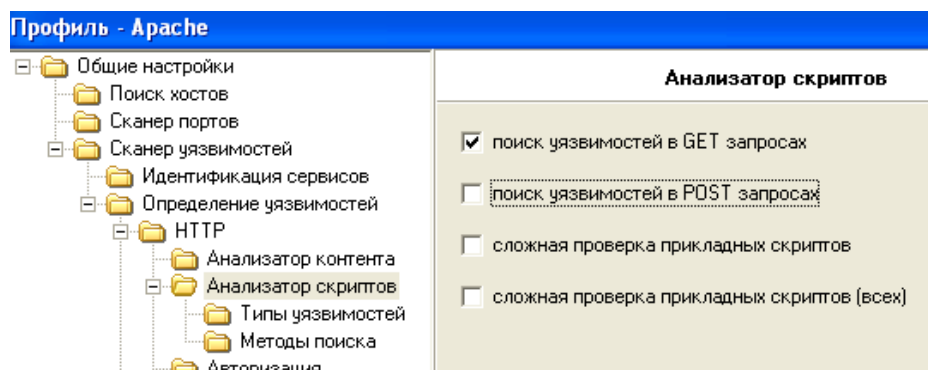
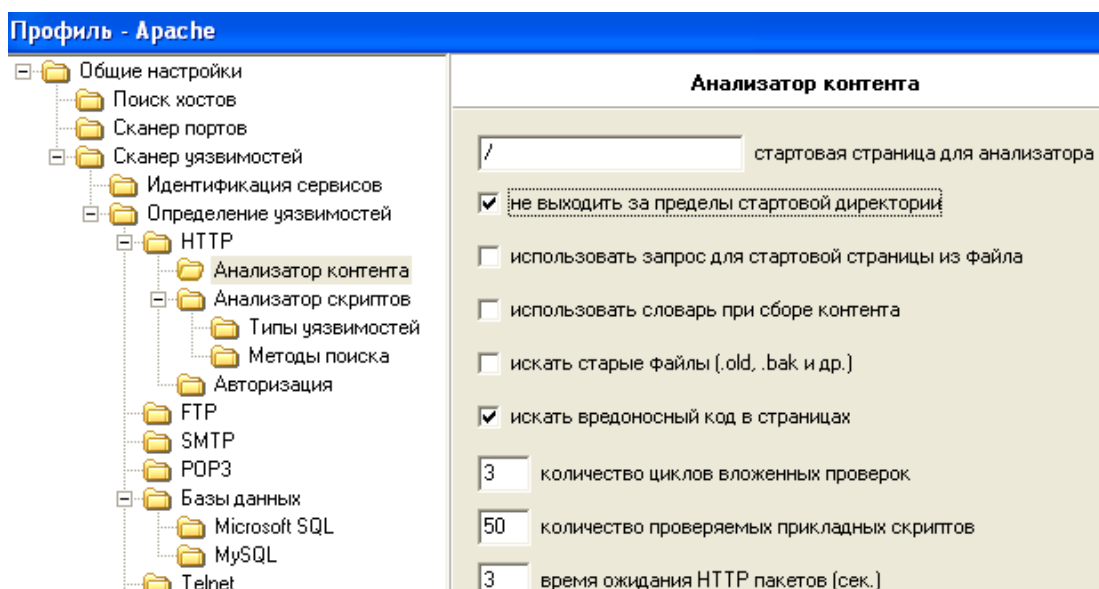
Цель работы: Обучение методам и средствам идентификации уязвимостей по косвенным признакам в сетевых приложениях КС.

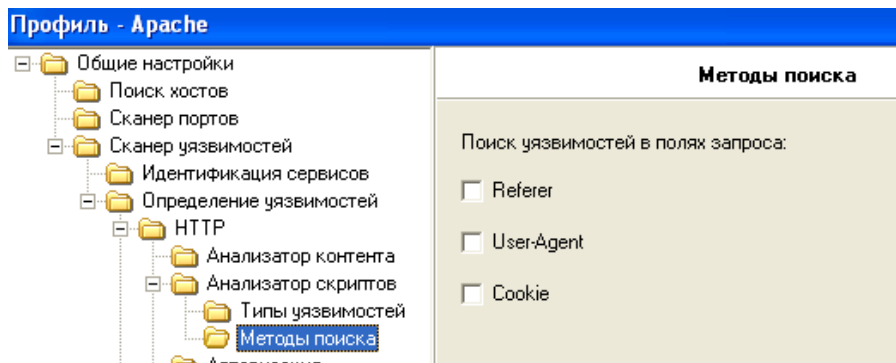
Ход работы

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 DoS-атаки», «Проверять на новые DoS-атаки».



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.





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
172.16.0.10

Информация

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

Параметры сканирования

Начало сканирования:	10:46:11 07.12.2022
Время сканирования:	00:00:16
Версия:	7.7 Demo Build 3100
Профиль:	Apache2.prf

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

```
(kali@kali)-[~]
$ nslookup
> server 172.16.0.1
Default server: 172.16.0.1
Address: 172.16.0.1#53
> set class=chaos
> set test=txt
*** Invalid option: test=txt
> version.bind
;; connection timed out; no servers could be reached
> authors.bind
;; connection timed out; no servers could be reached
> named -v
;; connection timed out; no servers could be reached
> rmp -q bind
;; connection timed out; no servers could be reached
> service named restart
;; connection timed out; no servers could be reached
```