

Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №5.
Идентификация уязвимостей сетевых приложений
по косвенным признакам

Проверил:

Грищенко В.В.

Студент МС – 42:

Кузнецов Ю.В.

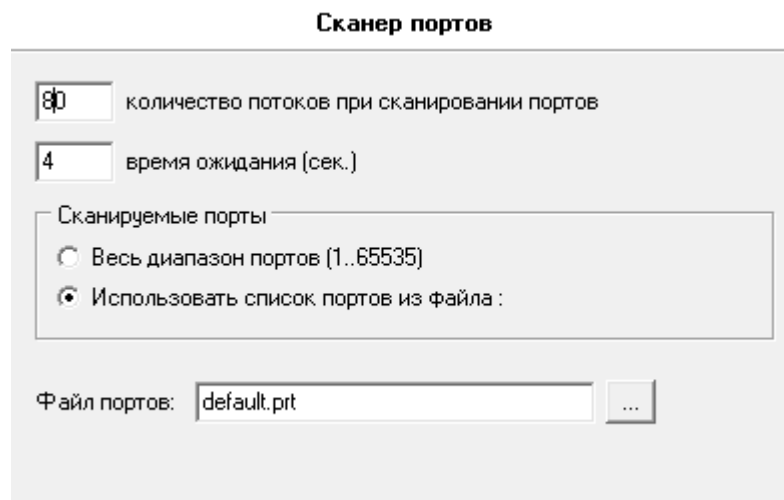
г. Гомель

Цель работы: Целью лабораторной работы является 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 DoS-атаки», «Проверять на новые DoS-атаки».

Сканер портов



80 количество потоков при сканировании портов

4 время ожидания (сек.)

Сканируемые порты

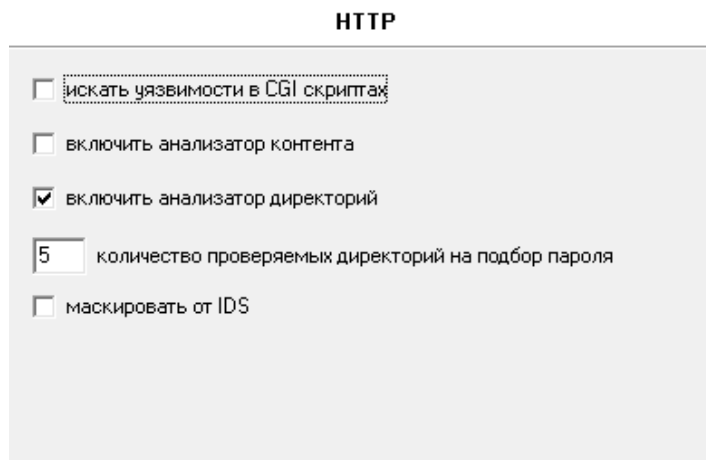
☐ Весь диапазон портов (1..65535)

☒ Использовать список портов из файла :

Файл портов: default.prt

Шаг 2. В секции «HTTP» 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.

HTTP



☒ искать уязвимости в CGI скриптах

☐ включить анализатор контента

☒ включить анализатор директорий

5 количество проверяемых директорий на подбор пароля

☐ маскировать от IDS

Анализатор контента

/ стартовая страница для анализатора

количество циклов вложенных проверок

количество проверяемых прикладных скриптов

☒ поиск уязвимостей в GET запросах

☐ поиск уязвимостей в POST запросах

☐ сложная проверка прикладных скриптов

Профиль - Apache

- Общие настройки
- Поиск хостов
- Сканер портов
- Сканер уязвимостей
 - Идентификация сервисов
 - Определение уязвимостей
 - HTTP
 - FTP**
 - POP3
 - SQL
 - Telnet
 - NetBIOS

FTP

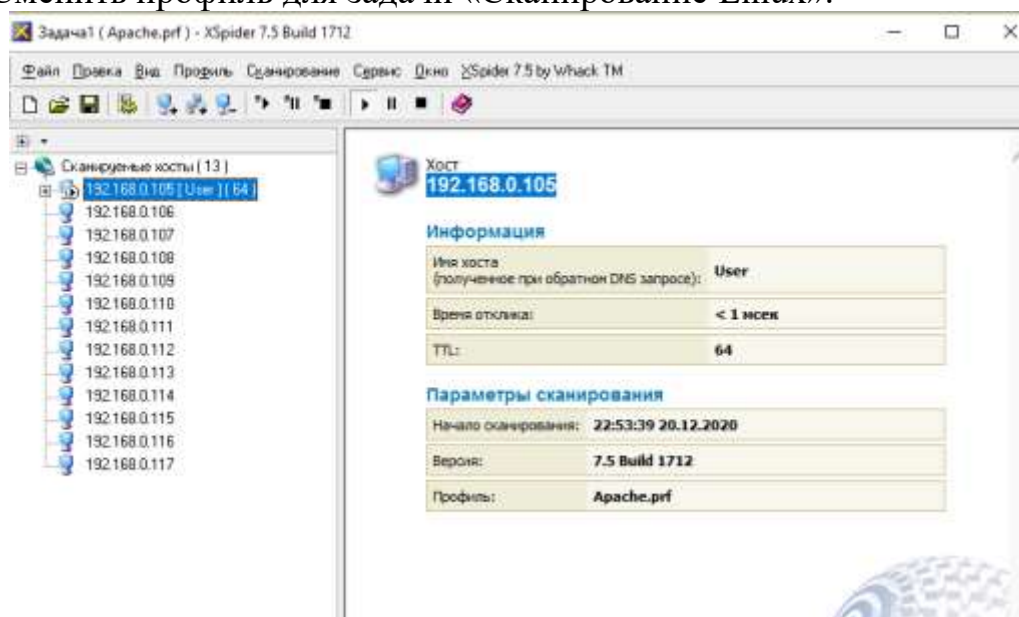
логин

пароль

☒ подбирать логин и пароль по словарю

☒ искать скрытые директории

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, используя средство nslookup:

C:>nslookup

>server 172.16.8.11

>set class=chaos

>set test=txt

>version.bind

Выполнить запрос authors.bind:

>authors.bind

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

Проверить установленную версию пакета bind: **rpm -q bind**

```
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53
> set class=chaos
> test=txt
;; connection timed out; no servers could be reached

> 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

> rpm -q bind
;; connection timed out; no servers could be reached
```