

Гомельский Государственный Университет
им. Ф. Скорины

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

Проверил:

Грищенко В.В.

Студент МС – 42:

Черненко А.В.

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».

The screenshot shows the 'Сканер портов' (Port Scanner) configuration window. On the left, a sidebar contains the text 'В мостей кация сервисов ние уязвимостей' and 'IDS'. The main panel has the title 'Сканер портов'. It contains a text input field with '80' and the label 'количество потоков при сканировании портов'. Below it is a text input field with '4' and the label 'время ожидания (сек.)'. A section titled 'Сканируемые порты' contains two radio buttons: 'Весь диапазон портов (1..65535)' and 'Использовать список портов из файла :', with the second one selected. At the bottom, there is a label 'Файл портов:' followed by a text input field containing 'default.prt' and a browse button with three dots.

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.

The screenshot shows the 'HTTP' configuration window. On the left, a sidebar contains the text 'об тей'. The main panel has the title 'HTTP'. It contains several checkboxes: 'искать уязвимости в CGI скриптах' (unchecked), 'включить анализатор контента' (unchecked), 'включить анализатор директорий' (checked), a text input field with '5' and the label 'количество проверяемых директорий на подбор пароля', and 'маскировать от IDS' (unchecked).

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

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».

Сканируемые hosts (13)

- 192.168.0.105 [User] (64)
- 192.168.0.106
- 192.168.0.107
- 192.168.0.108
- 192.168.0.109
- 192.168.0.110
- 192.168.0.111
- 192.168.0.112
- 192.168.0.113
- 192.168.0.114
- 192.168.0.115
- 192.168.0.116
- 192.168.0.117

Хост
192.168.0.105

Информация

Имя хоста (полученное при обратном DNS запросе):	User
Время отклика:	< 1 мсек
TTL:	64

Параметры сканирования

Начало сканирования:	22:53:39 20.12.2020
Версия:	7.5 Build 1712
Профиль:	Apache.prf

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**

```
breof@breof-80ru:~$ nslookup
> 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
```