Министерство образования Республики Беларусь

Учреждение образования

Отчёт по лабораторной работе №5

«Идентификация уязвимостей сетевых приложений по косвенным признакам»

Выполнил:

Студент группы МС-42

Кнышев Н.В.

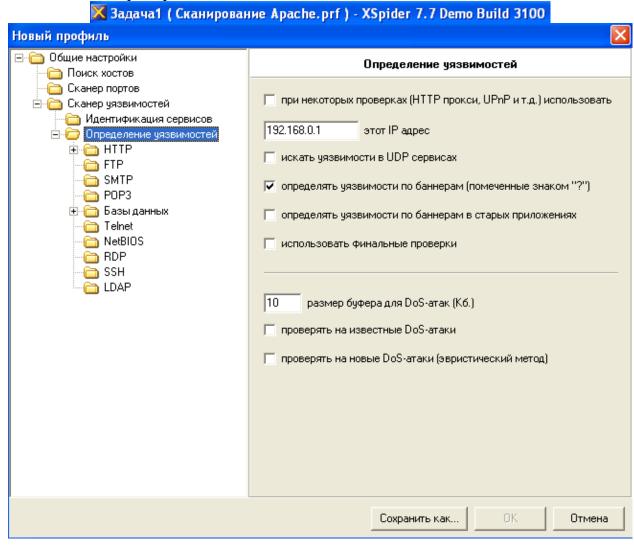
Проверил: Грищенко В.В.

Лабораторная работа №5

Цель работы: 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 DoSатаки», «Проверять на новые DoS-атаки».



Шаг 2. 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. Профиль - Сканирование Apache 🔀 Профиль - Сканирование Apache шттр Анализатор контента □ Общие пастроим

Поиск хостов

Сканер портов

Сканер узавиностей

Маритизикация сервисов

Определение узавиностей

Тоределение узавиностей 🗸 не выходить за пределы стартовой директории ✓ искать уязвимости в СGI скриптах (поиск по содержимому) включить анализатор контента Анализатор контента
 Анализатор скриптов
 Типы уязвимостей
 Методы поиска Анализатор скриптов
 Типы уязвимостей
 Методы поиска
 А-горугания ✓ искать межсайтовый скриптинг в методах Trace и Track □ uckats ctanse файлы (old_bak u.m.) — (a) Авторизация (b) FTP искать вредоносный код в страницах пригие проверки SMTP 5 количество проверяемых директорий на подбор пароля 3 количество циклов вложенных проверог 🚊 🦲 Базы данных 🚊 🦲 Базы данных Microsoft SQL
MySQL
Telnet
NetBIOS 50 количество проверяемых прикладных скриптов Microsoft SQL
MySQL
Telnet 3 время ожидания HTTP пакетов (сек.) NetBIOS A RDP a RDP SSH LDAP LDAP Сохранить как... ОК Отмена Профиль - Сканирование Apache Профиль - Сканирование Apache Поиск хостов Сканер портов
 Сканер уязвимостей
 Мдентификация сервисов Сканер портов Поиск уязвимостей в полях запроса Идентификация сервисов □ SQL инъекция ☐ Referen 🖃 🦰 Определение уязвимостей Определение уязвимостей НТТР 🗌 удаленное выполнение команд ☐ User-Agent Анализатор контента Анализатор контента ⇒ Анализатор скриптов
 ⇒ Типы уязвимостей
 ⇒ Методы поиска 🖹 🦲 Анализатор скриптов Cookie Server Side Includes (SSI) SMTP POP3 ☐ HTTP Response Splitting POP3 POP3

Basia данных

Microsoft SQL

MySQL

Telnet

NetBIOS

RDP

SSH Базы данных

Місгозоft SQL

МуSQL

Telnet выполнение кода, взятого с удаленного сервера NetBIOS
RDP
SSH
LDAP

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, использую средство 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
> service named restart
;; connection timed out; no servers could be reached
```

Вывод: в ходе лабораторной работы были изучены методы и средства идентификации уязвимостей по косвенным признакам в сетевых приложениях КС, выполнена идентификация уязвимостей сетевых служб DNS, HTTP и SSH по косвенным признакам с помощью сканера XSpider.