Министерство образования Республики Беларусь Учреждение образования "Гомельский государственный университет им. Франциска Скорины"

Отчёт по лабораторной работе №5 «Идентификация уязвимостей сетевых приложений по косвенным признакам»

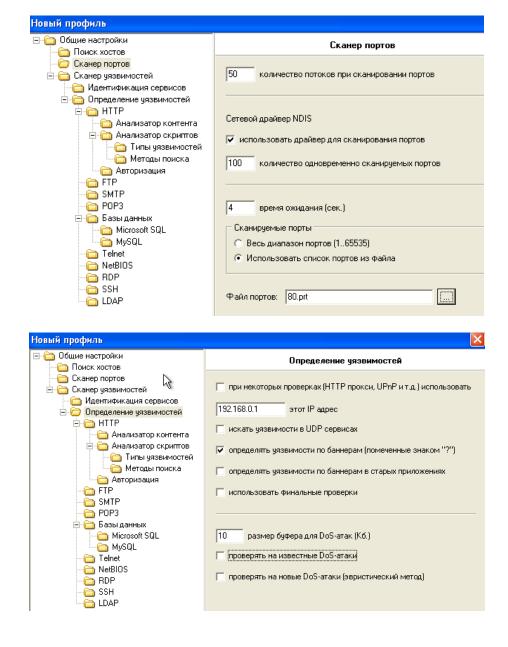
Выполнил: Студент группы МС-42 Созинов Л.В. Проверил: Грищенко В.В.

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.

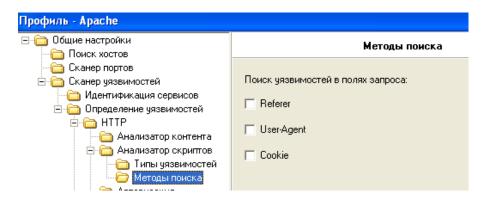
Ход работы

1. Создадим профиль сканирования «Сканирование Арасhe». 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 «НТТР» 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.

| Профиль - Apache | | |
|---|-------------------------|---|
| □ □ Общие настройки □ □ □ Сканер портов □ □ □ Сканер уязвимостей □ □ □ Идентификация сервисов □ □ □ НТТР □ □ Анализатор контента □ □ □ Анализатор скриптов □ □ Типы уязвимостей □ Методы поиска □ □ Ваторизация □ FTP □ SMTP □ POP3 □ □ Базы данных □ Microsoft SQL □ MySQL □ Telnet | | Анализатор контента стартовая страница для анализатор не выходить за пределы стартовой директории использовать запрос для стартовой страницы из файла использовать словарь при сборе контента искать старые файлы (.old, .bak и др.) искать вредоносный код в страницах количество циклов вложенных проверок количество проверяемых прикладных скриптов время ожидания НТТР пакетов (сек.) |
| Профиль - Арасhe □ Общие настройки Поиск хостов Сканер портов □ Сканер уязвимостей Идентификация сервисов □ Определение уязвимостей □ НТТР □ Анализатор контен □ Анализатор скрит □ Типы уязвимостей Методы поиска | й -па гов стей | Анализатор скриптов ✓ поиск уязвимостей в GET запросах □ поиск уязвимостей в POST запросах □ сложная проверка прикладных скриптов □ сложная проверка прикладных скриптов (всех) |
| Профиль - Арасhе □ ○ Общие настройки ○ Поиск хостов ○ Сканер портов ○ Сканер уязвимостей ○ Идентификация сервисов ○ Попеделение уязвимостей ○ НТТР ○ Анализатор контента ○ Анализатор скриптов ○ Типы уязвимосте ○ Методы поиска ○ Авторизация ○ FTP ○ SMTP ○ SMTP ○ POP3 ○ Базы данных ○ Microsoft SQL | В | Типы уязвимостей в прикладных скриптах: SQL инъекция удаленное выполнение команд просмотр произвольных файлов межсайтовый скриптинг (XSS) Server Side Includes (SSI) HTTP Response Splitting выполнение кода, взятого с удаленного сервера |



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».



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

```
(skali⊕kali)-[~]
> 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
```