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

Отчёт по лабораторной работе №6

«Идентификация уязвимостей на основе тестов»

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

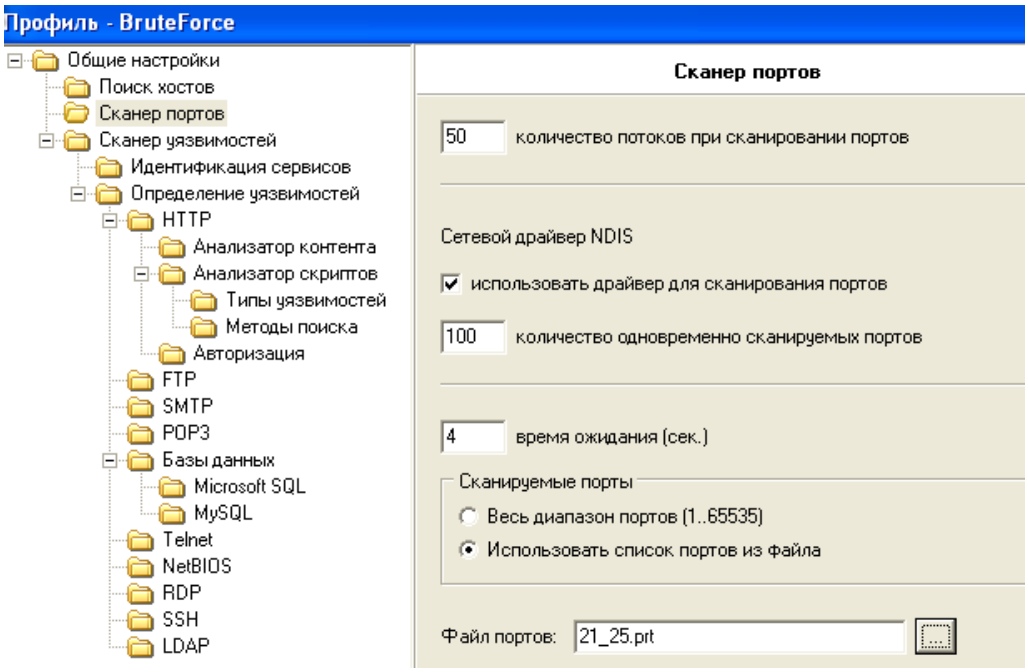
2022

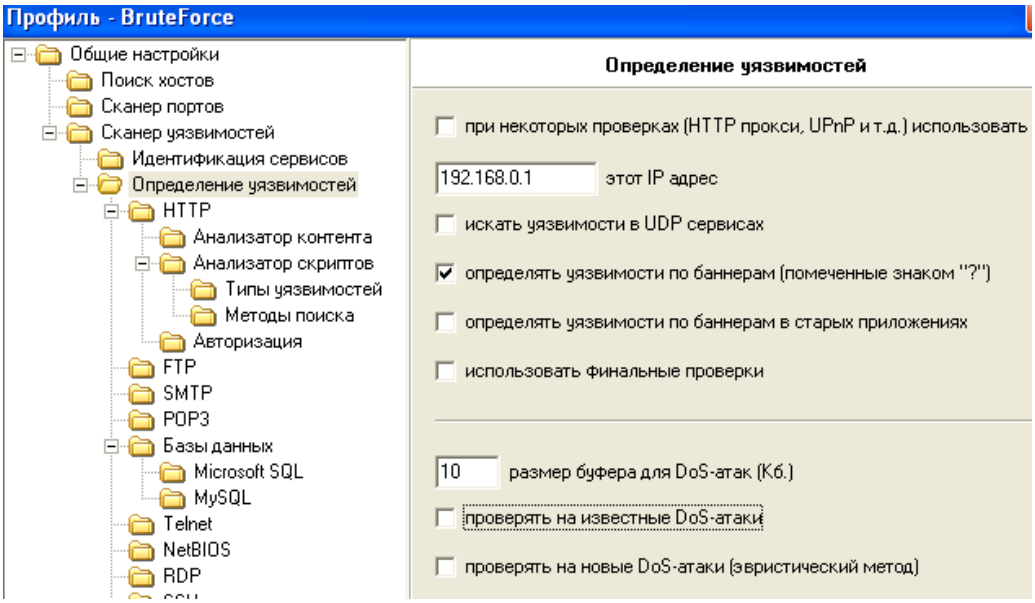
Лабораторная работа №6
Идентификация уязвимостей на основе тестов

Цель работы: Обучение методам и средствам идентификации уязвимостей на основе тестов.

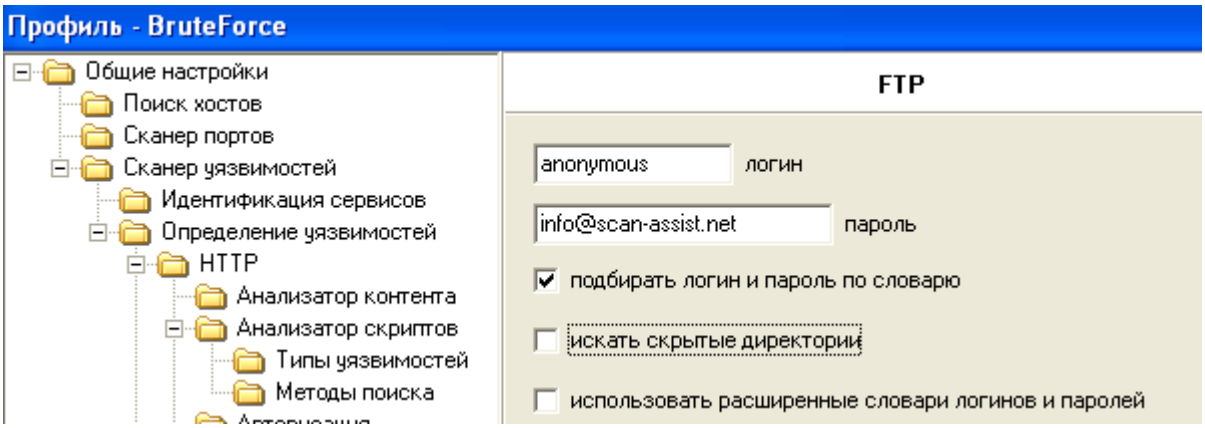
Ход работы

1. Создадим новый профиль сканирования с именем «BruteForce». Перечень сканируемых портов ограничим портами служб FTP (21) и SMTP (25). Отключим сканирование служб UDP, в секции «Определение уязвимостей» отключим опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».



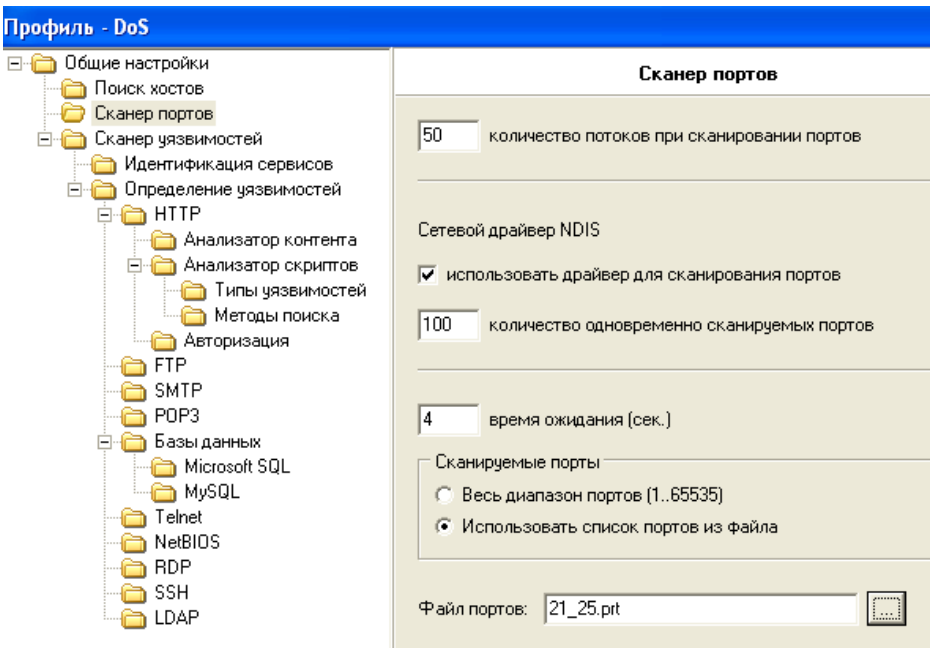


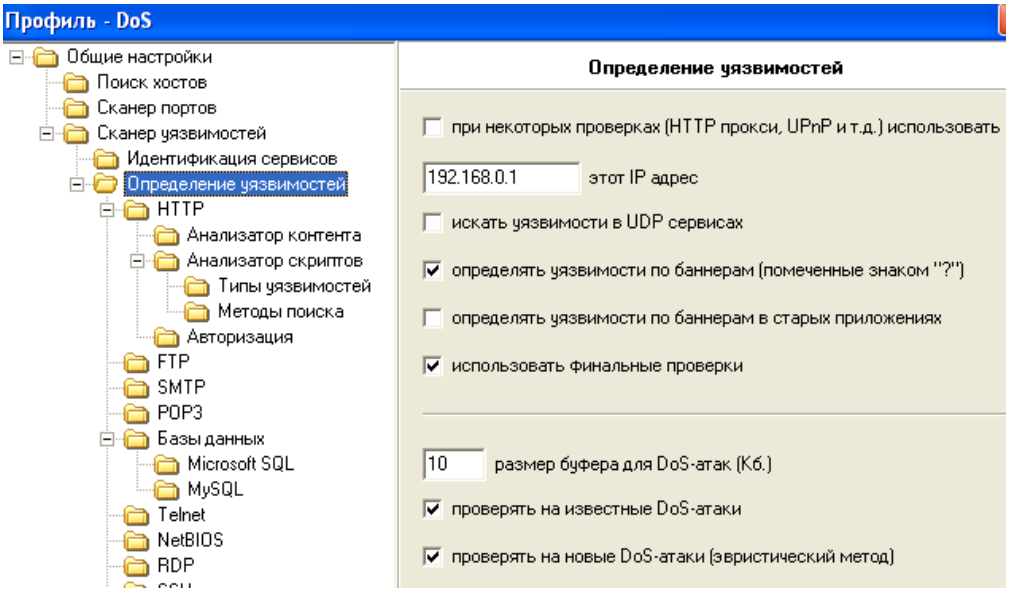
2. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключим опцию «Искать скрытые директории». Включим опцию «Подбирать учётные записи», выберем ранее созданные словари логинов и паролей. Сохраним профиль сканирования.



3. Создадим новую задачу «Подбор паролей», выбрав созданный ранее профиль сканирования «BruteForce». Выполним сканирование сервера. Проанализируем результаты. Убедимся в подборе пароля к службам FTP и SMTP.

4. Создадим профиль сканирования «DoS». В список сканируемых портов добавим TCP порты 21 и 25. Отключим сканирование служб UDP. Включим опции «Искать уязвимости». В секции «Определение уязвимостей» включим опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключим опцию «Подбирать учетные записи».





5. Создадим задачу «Финальные проверки», используя профиль «DoS». Выполним сканирование.