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

Отчёт по лабораторной работе №6

«Идентификация уязвимостей на основе тестов»

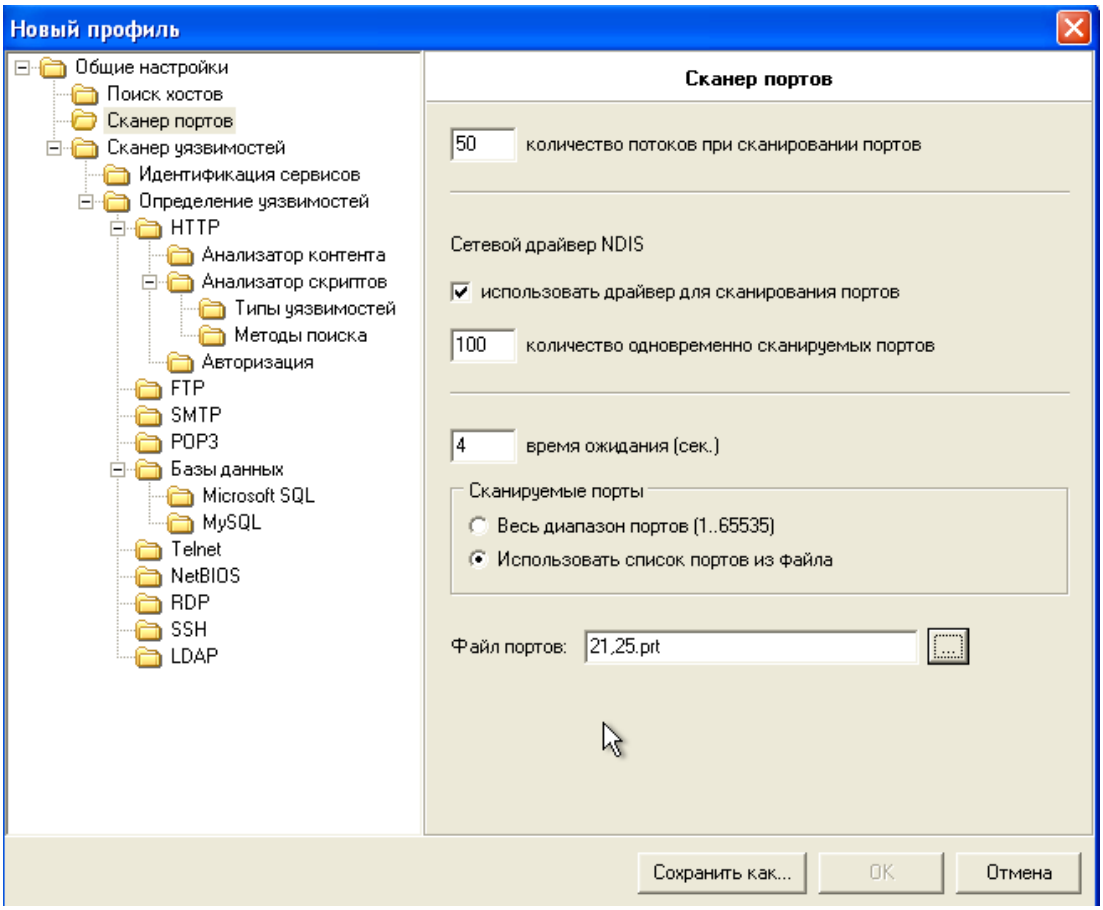
Выполнил:
Студент группы МС-42
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

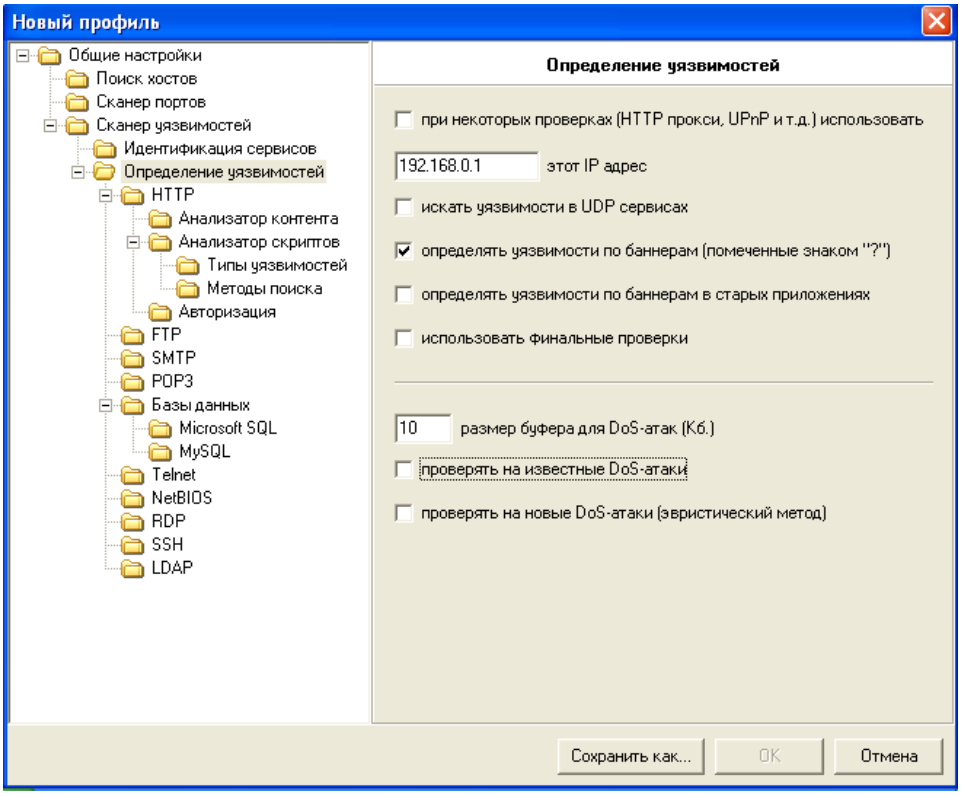
2022

Цель работы: обучение методам и средствам идентификации уязвимостей наоснове тестов.

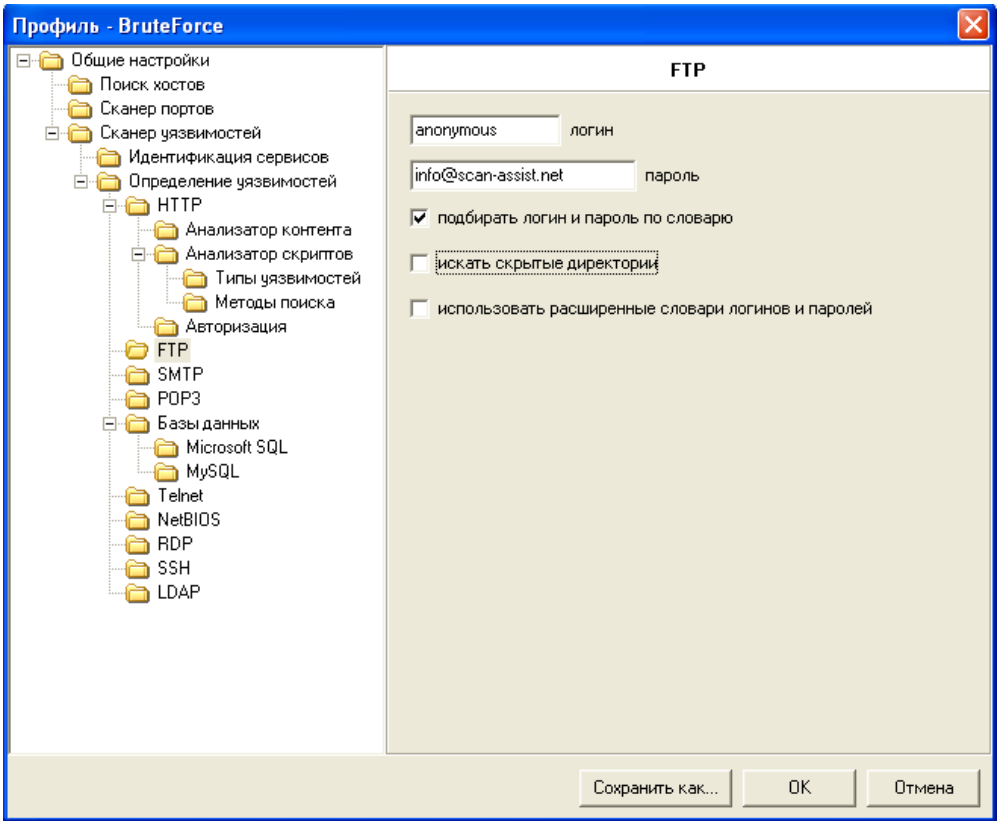
Ход работы.

Шаг 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».



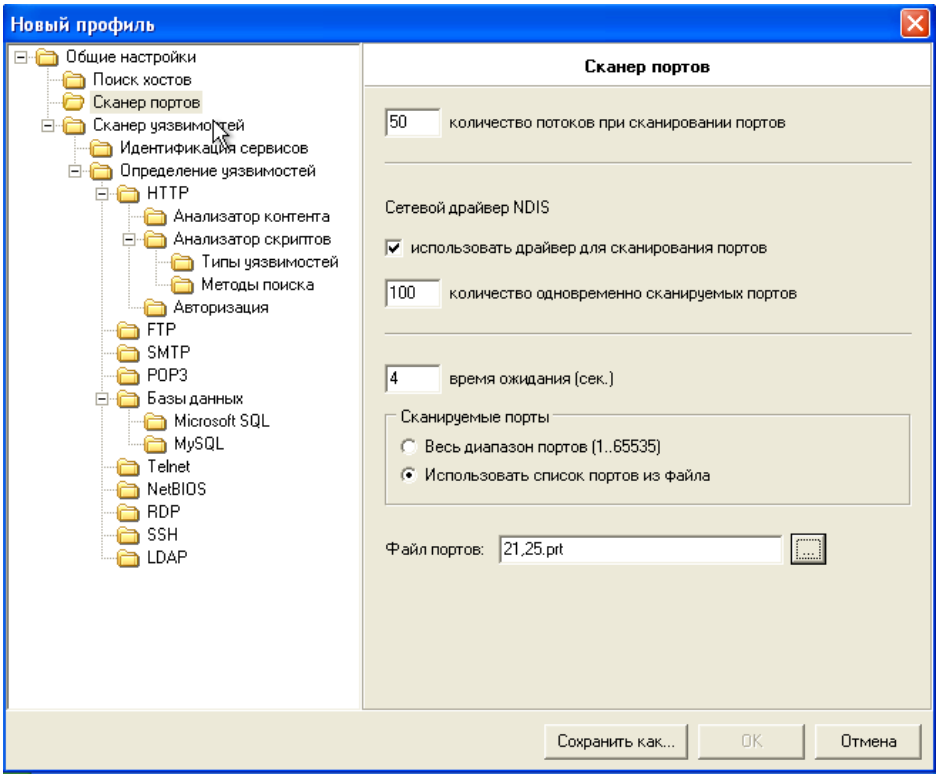


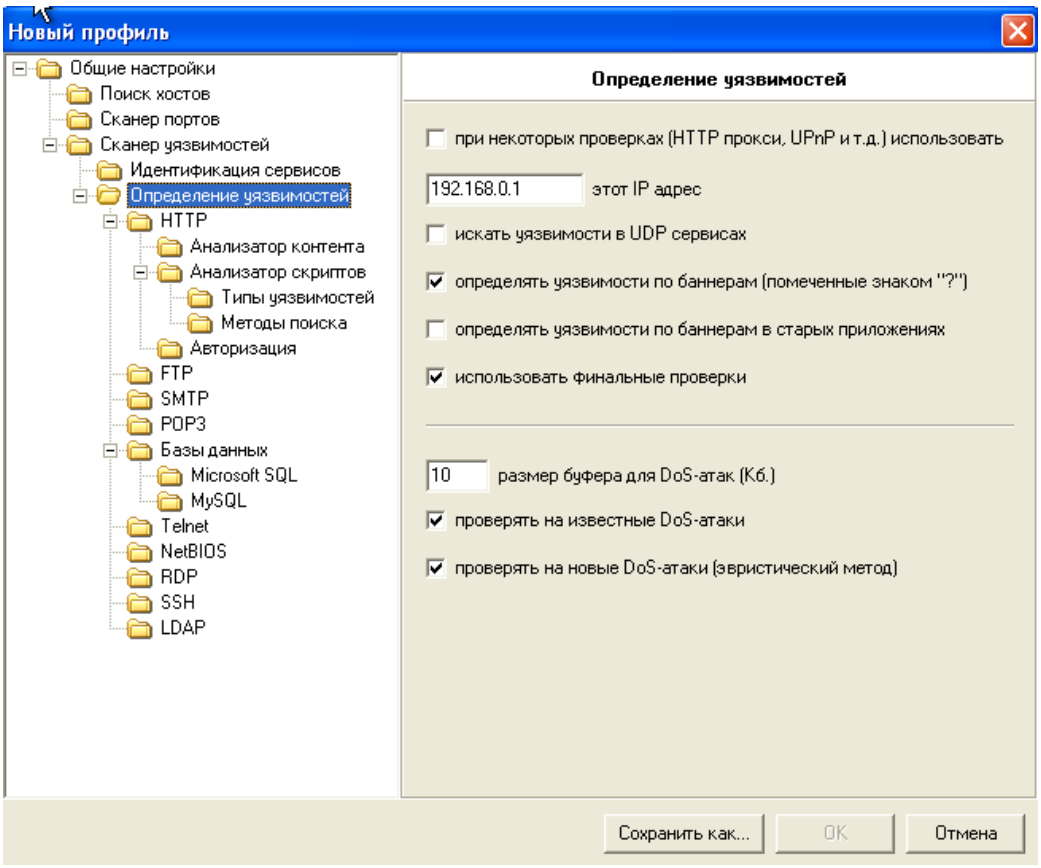
Шаг 2. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключим опцию «Искать скрытые директории». Включим опцию «Подбирать учётные записи», выберем ранее созданные словари логинов ипаролей. Сохраним профиль сканирования.



Шаг 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.

Шаг 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».





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

Вывод: в ходе лабораторной работы познакомились с методами и средствами идентификации уязвимостей на основе тестов.