Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №6.
Идентификация уязвимостей на основе тестов

Проверил:
Грищенко В.В.

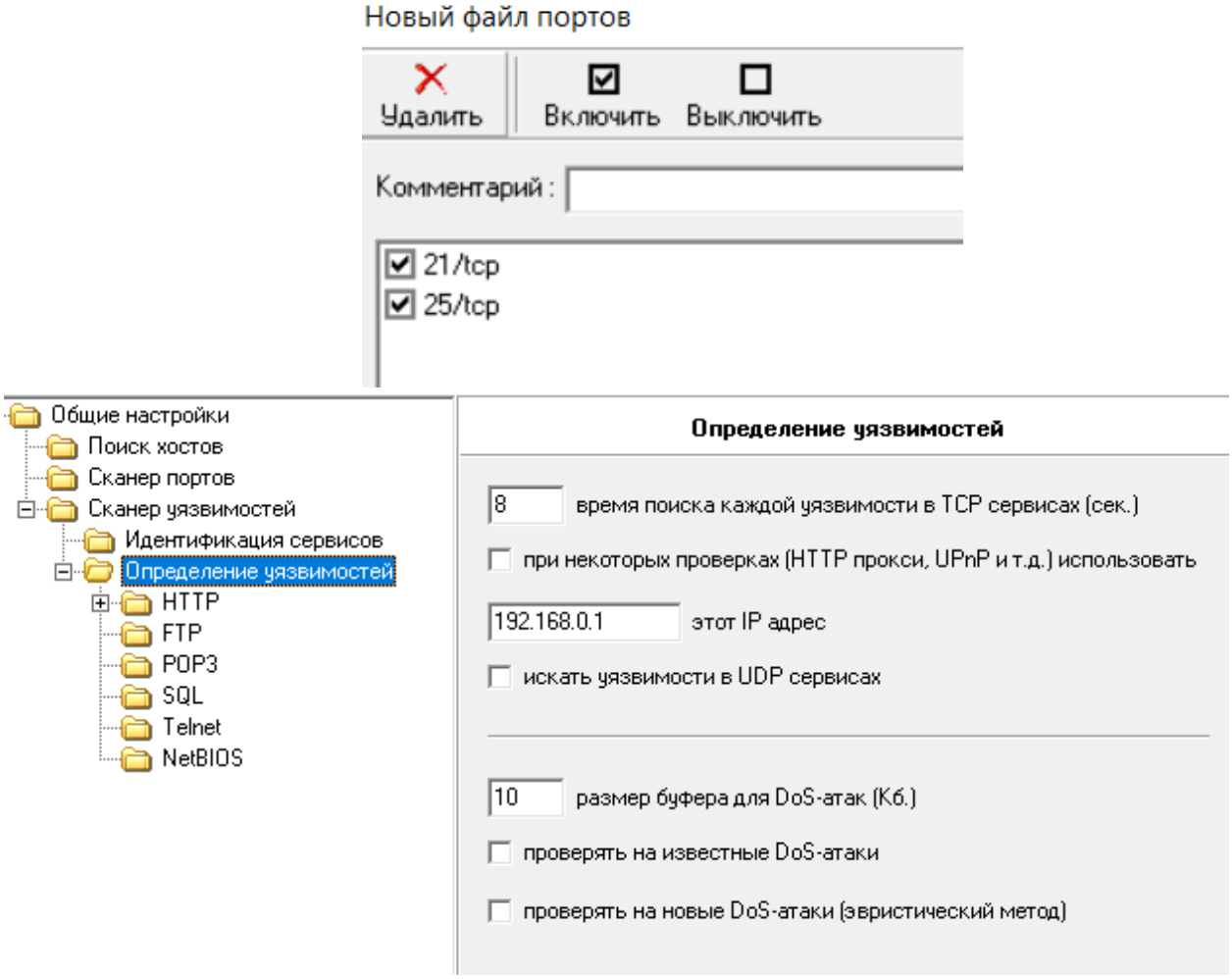
Студент МС – 42:
Кузнецов Ю.В.

г. Гомель

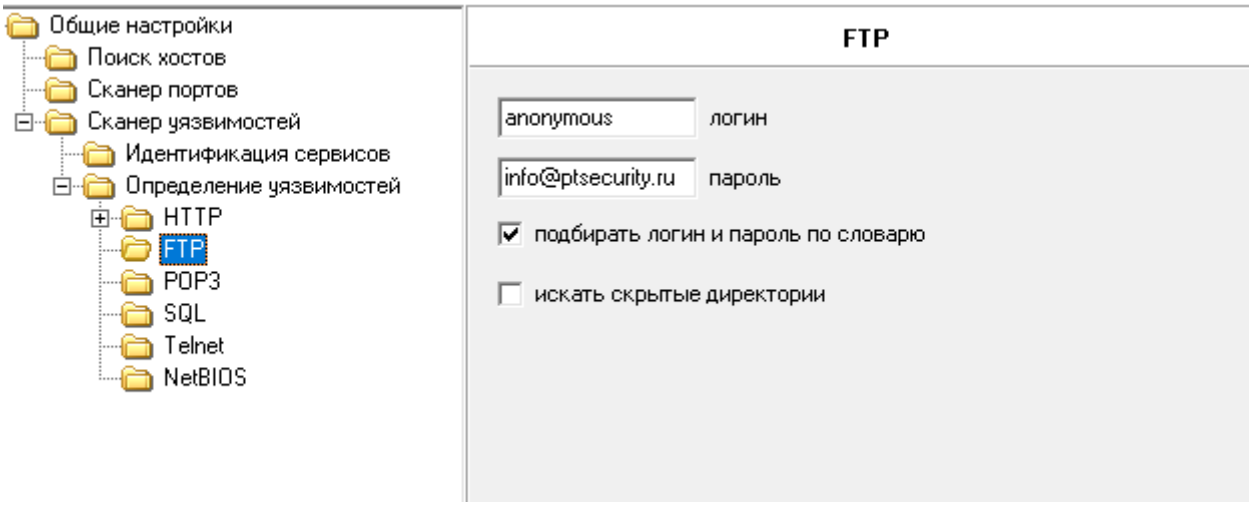
Цель работы: Целью лабораторной работы является обучение методам и средствам идентификации уязвимостей на основе тестов.

Постановка задачи: выполнить идентификацию уязвимостей и подбор учетных записей с использованием сканера безопасности XSpider.

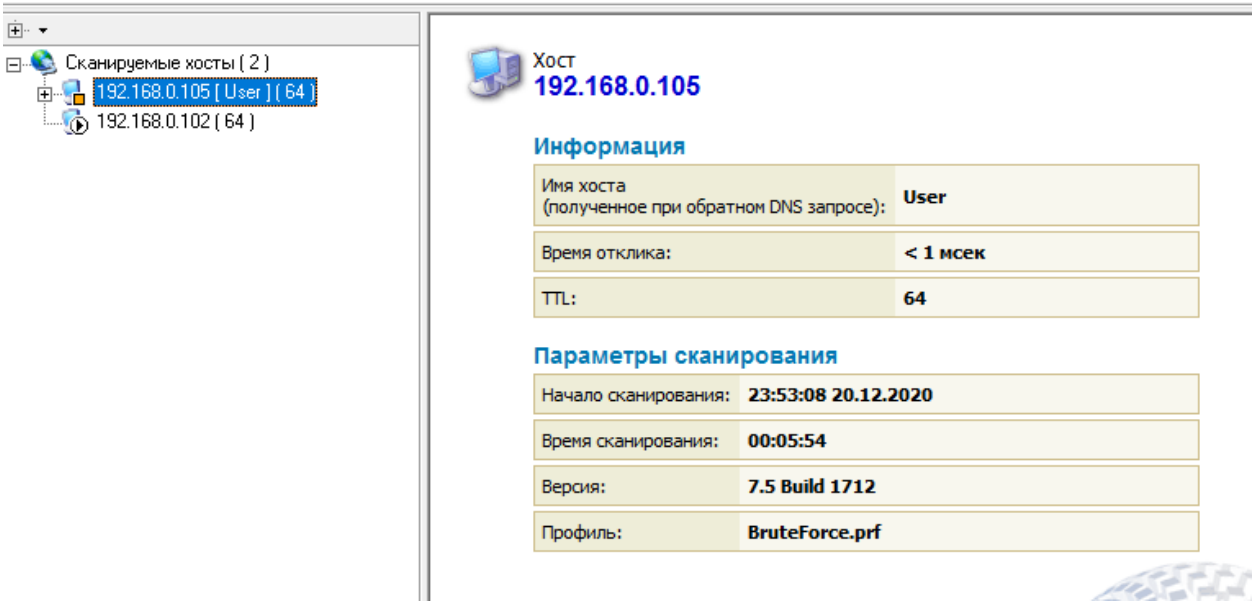
Шаг 1. Создать новый профиль сканирования с именем «BruteForce». Перечень сканируемых портов ограничить портами служб FTP (21) и SMTP (25). Отключить сканирование служб UDP, в секции «Определение уязвимостей» отключить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять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



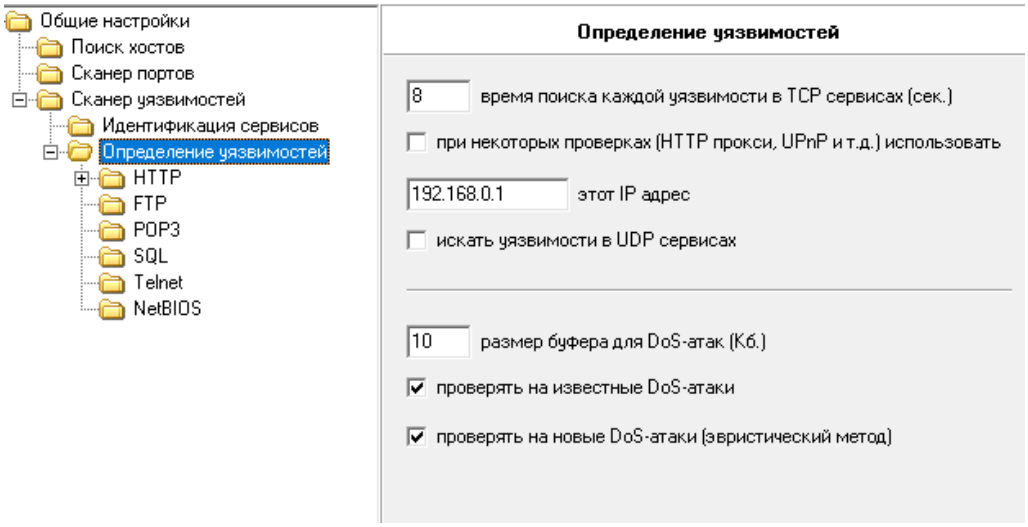
Шаг 2. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключить опцию «Искать скрытые директории». Включить опцию «Подбирать учётные записи», выбрать ранее созданные словари логинов и паролей. Сохранить профиль сканирования.



Шаг 3. Создать новую задачу «Подбор паролей», выбрав созданный ранее профиль сканирования «BruteForce». Выполнить сканирование сервера S2. Проанализировать результаты. Убедиться в подборе пароля к службам FTP и SMTP.



Шаг 4. Создать профиль сканирования «DoS». В список сканируемых портов добавить TCP порты 21 и 25. Отключить сканирование служб UDP. Включить опции «Искать уязвимости». В секции «Определение уязвимостей» включить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключить опцию «Подбирать учетные записи».



Шаг 5. Создать задачу «Финальные проверки», используя профиль «DoS». Выполнить сканирование.