Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Отчёт по лабораторной работе №6
«Идентификация уязвимостей на основе тестов»

Выполнил студент группы МС-42: Казак И.В.

Проверил:

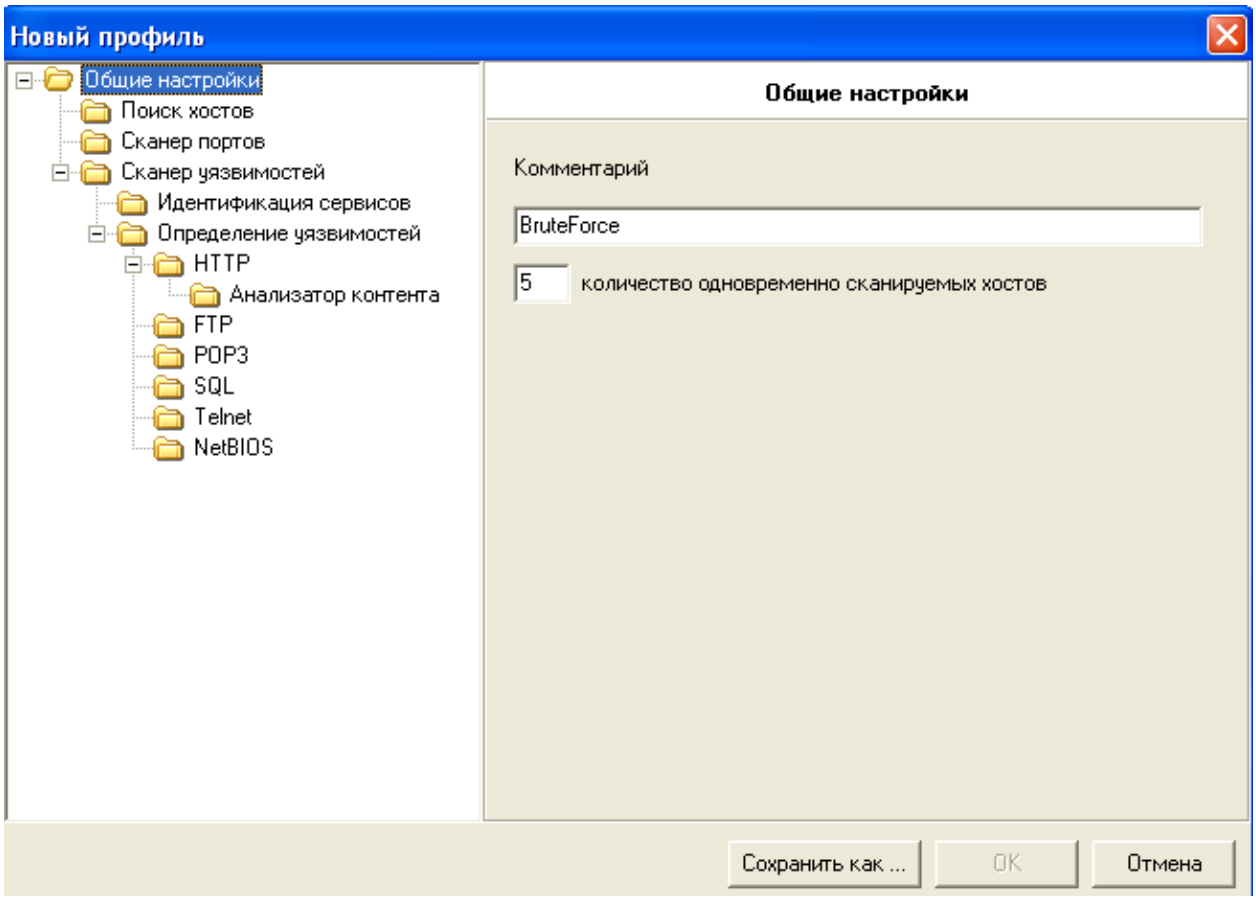
Старший преподаватель Грищенко В.В.

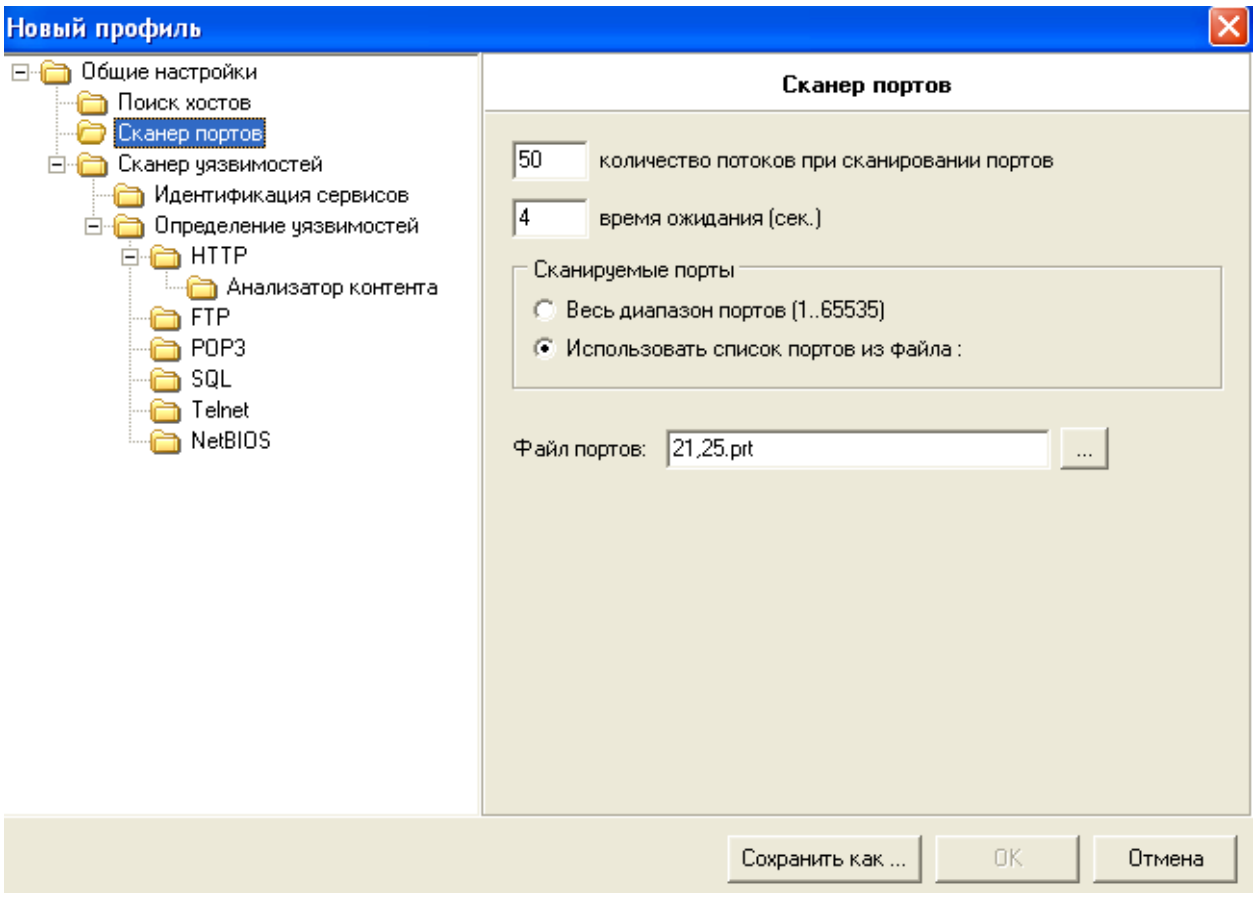
Гомель 2022

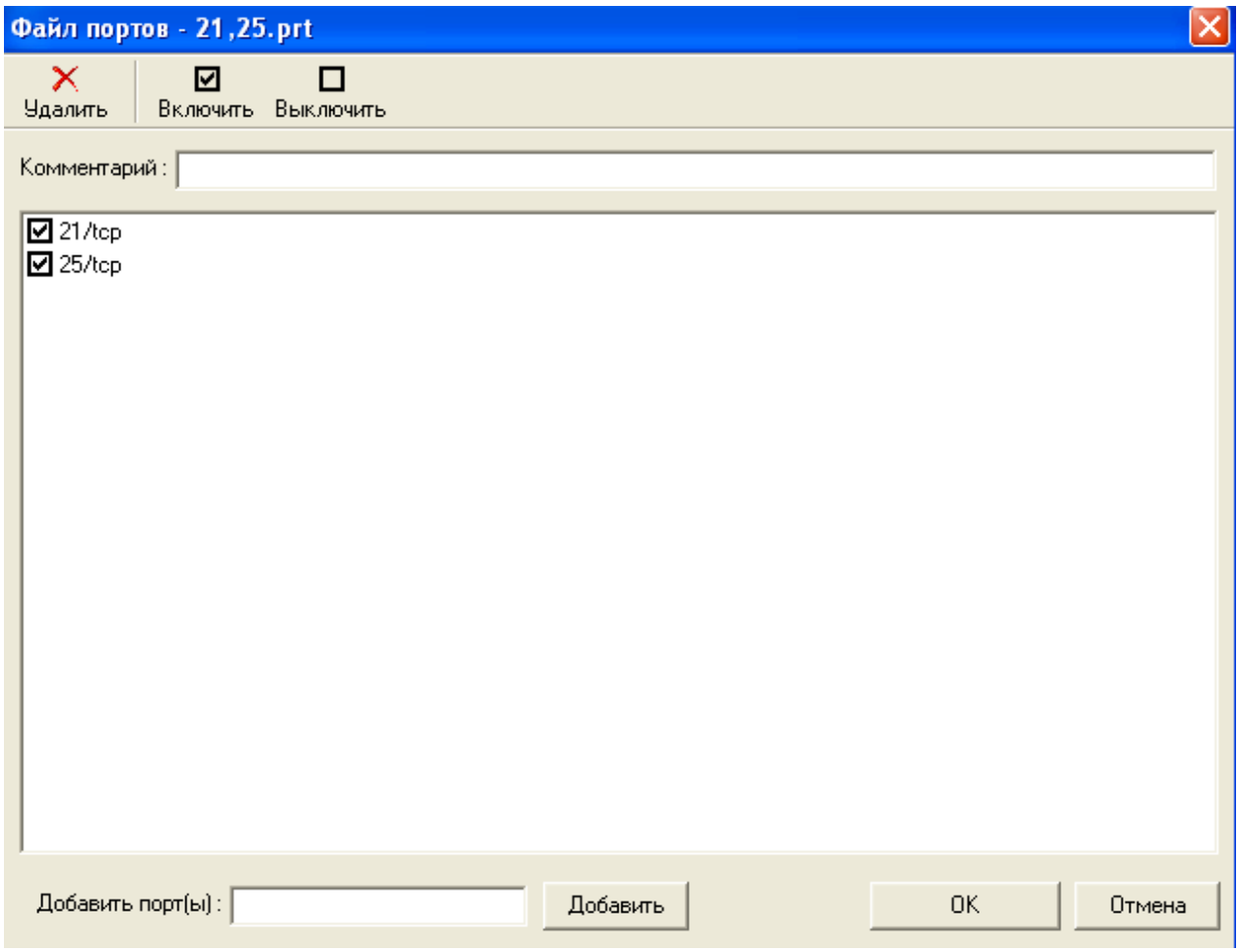
Цель работы: обучение методам и средствам идентификации уязвимостей на основе тестов.

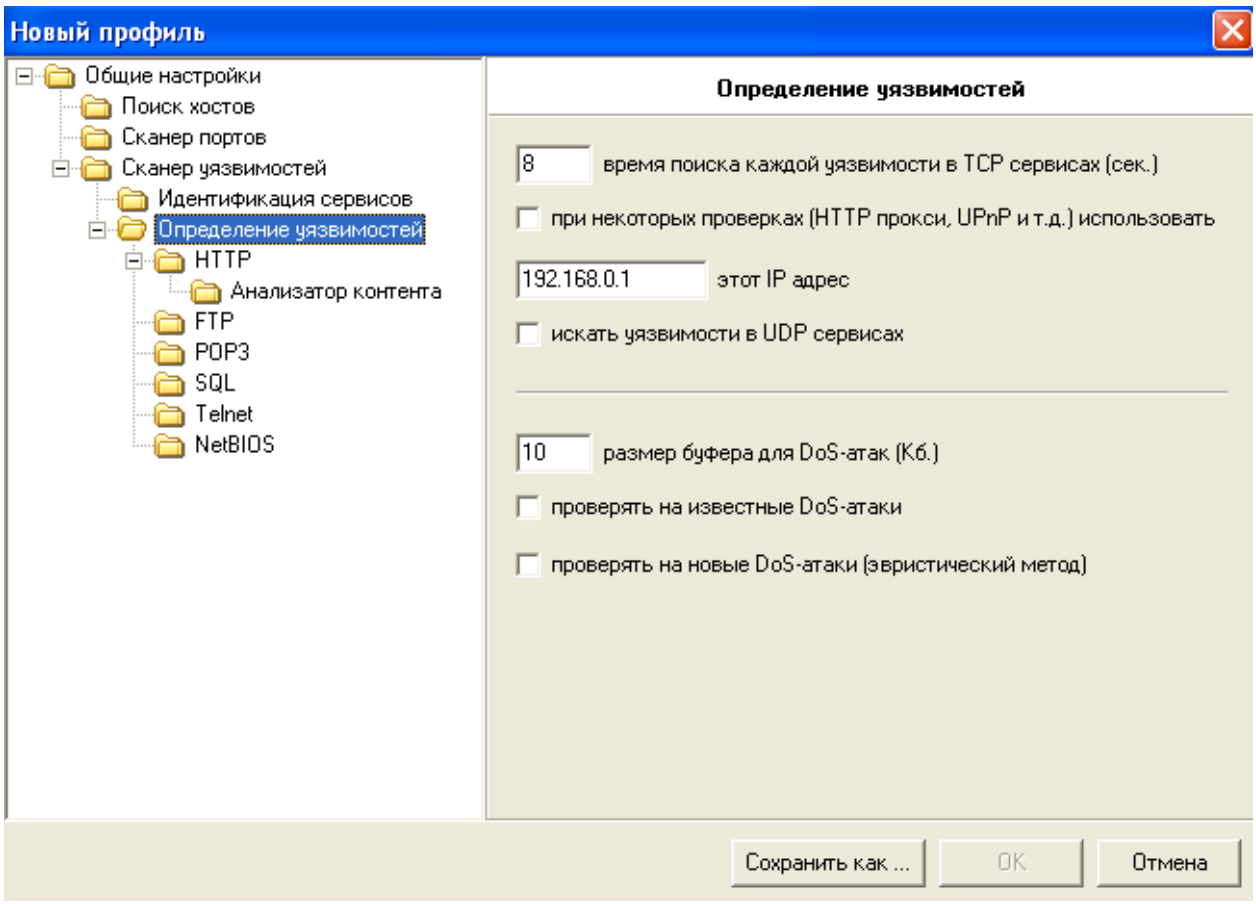
Ход работы.

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».

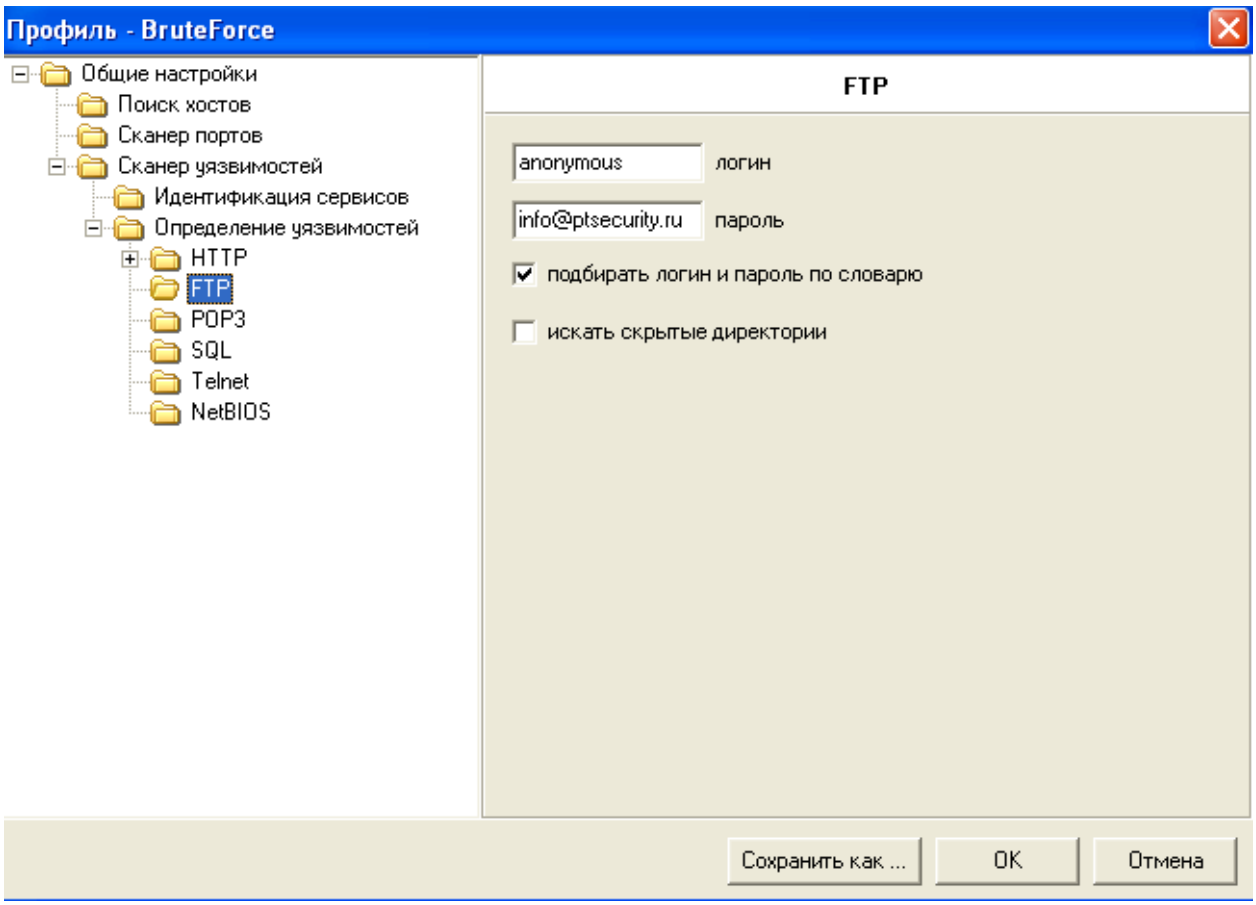



Новый профиль
Общие настройки
Поиск хостов
Сканер портов
Сканер уязвимостей
Идентификация сервисов
Определение уязвимостей
HTTP
Анализатор контента
FTP
POP3
SQL
Telnet
NetBIOS
Сканер портов
50
количество потоков при сканировании портов
4
время ожидания (сек.)
Сканируемые порты
Весь диапазон портов (1..65535)
Использовать список портов из файла :
Файл портов:
21,25.prt
...
Сохранить как ...
OK
Отмена

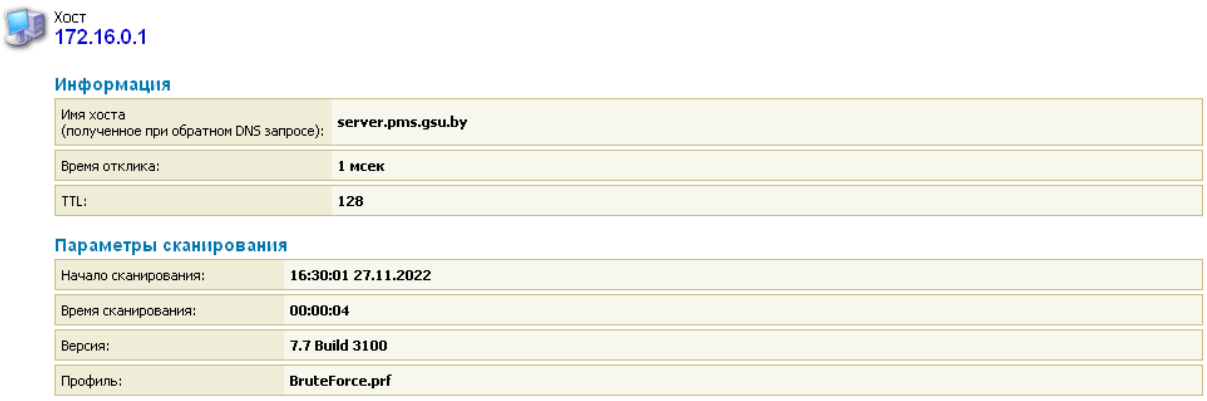

Файл портов - 21,25.prt
Удалить
Включить
Выключить
Комментарий :
21/tcp
25/tcp
Добавить порт(ы) :
Добавить
OK
Отмена



Шаг 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.



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.



Хост
172.16.0.1

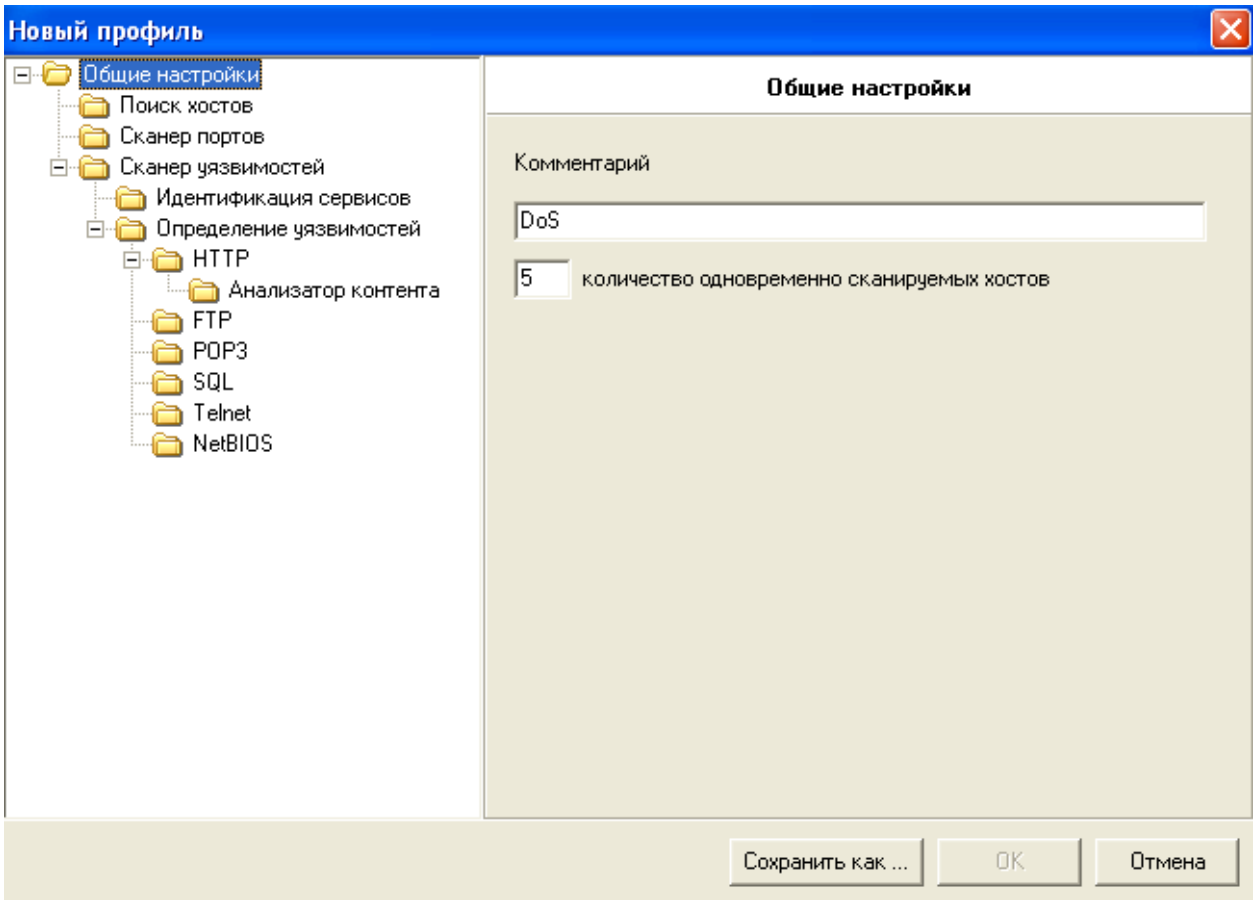
Информация

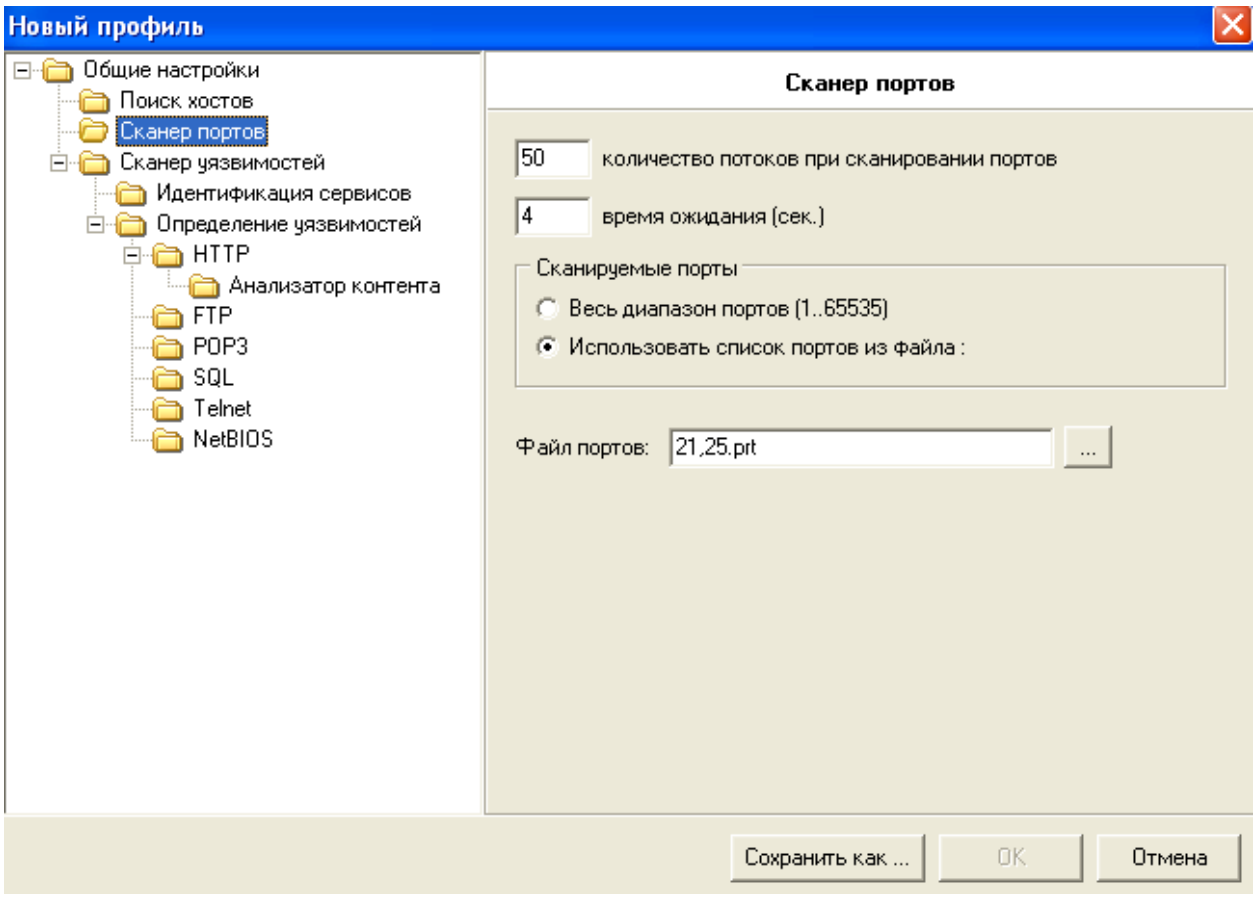
Имя хоста (полученное при обратном DNS запросе):	**server.pms.gsu.by**
Время отклика:	**1 мсек**
TTL:	**128**

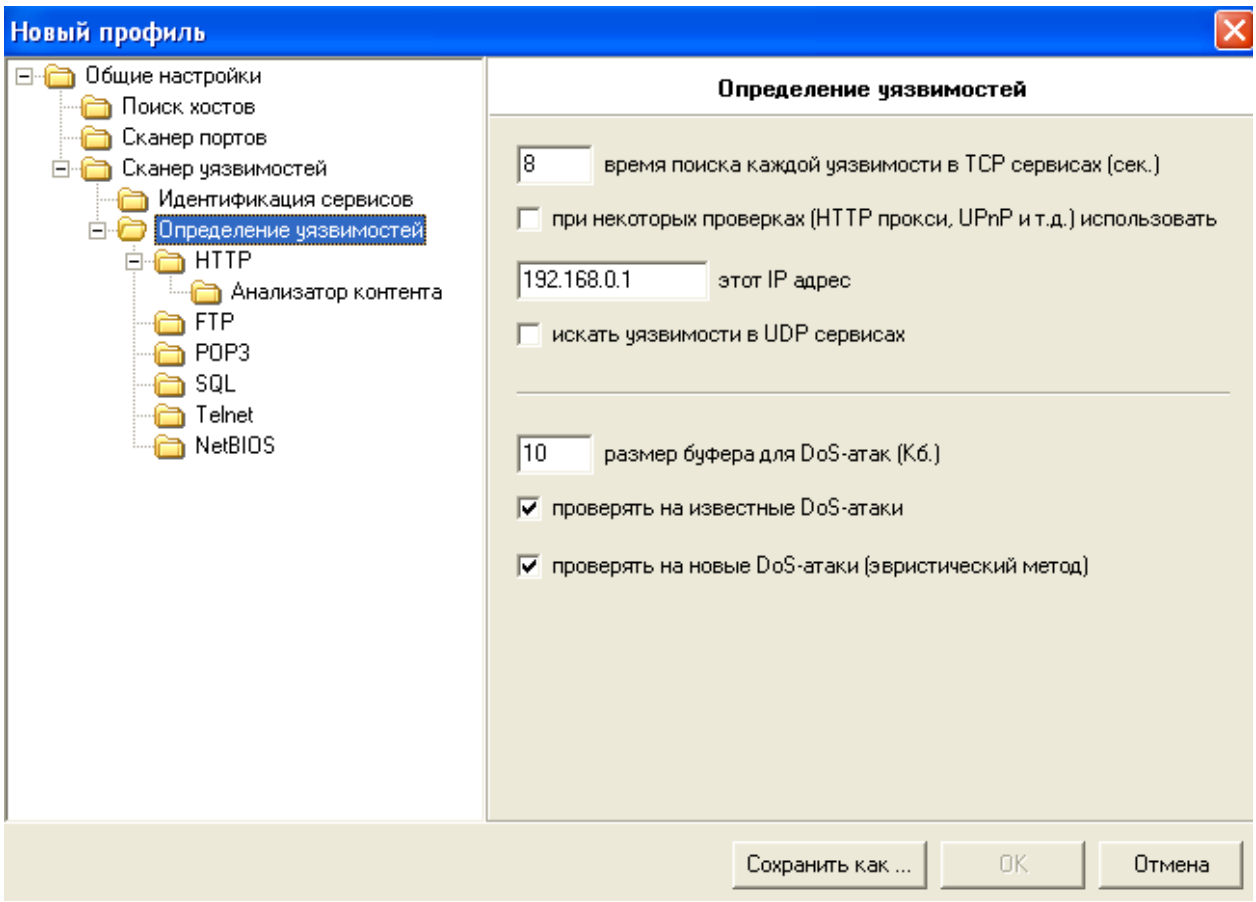
Параметры сканирования

Начало сканирования:	**16:30:01 27.11.2022**
Время сканирования:	**00:00:04**
Версия:	**7.7 Build 3100**
Профиль:	**BruteForce.prf**

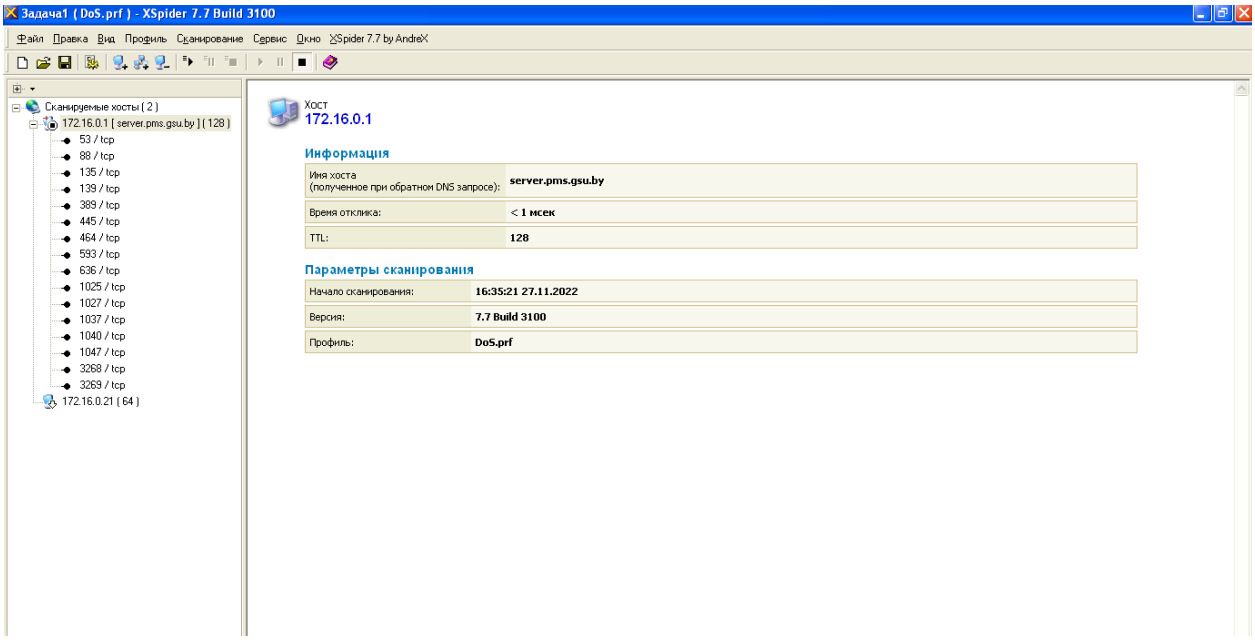
Шаг 4. Создадим профиль сканирования «DoS». В список сканируемых портов добавим TCP порты 21 и 25. Отключим сканирование служб UDP. Включим опции «Искать уязвимости». В секции «Определение уязвимостей» включим опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключим опцию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




Новый профиль
Общие настройки
Поиск хостов
Сканер портов
Сканер уязвимостей
Идентификация сервисов
Определение уязвимостей
HTTP
Анализатор контента
FTP
POP3
SQL
Telnet
NetBIOS
Сканер портов
50
количество потоков при сканировании портов
4
время ожидания (сек.)
Сканируемые порты
Весь диапазон портов (1..65535)
Использовать список портов из файла :
Файл портов:
21,25.prt
...
Сохранить как ...
OK
Отмена


Новый профиль
Общие настройки
Поиск хостов
Сканер портов
Сканер уязвимостей
Идентификация сервисов
Определение уязвимостей
HTTP
Анализатор контента
FTP
POP3
SQL
Telnet
NetBIOS
Определение уязвимостей
8
время поиска каждой уязвимости в TCP сервисах (сек.)
при некоторых проверках (HTTP прокси, UPnP и т.д.) использовать
192.168.0.1
этот IP адрес
искать уязвимости в UDP сервисах
10
размер буфера для DoS-атак (Кб.)
проверять на известные DoS-атаки
проверять на новые DoS-атаки (эвристический метод)
Сохранить как ...
OK
Отмена

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



Вывод: в ходе лабораторной работы познакомились, а также воспользовались методами и средствами идентификации уязвимостей на основе тестов.