Гомельский Государственный Университет им. Ф. Скорины

**Отчёт по лабораторной работе № 7**

**Особенности идентификации уязвимостей ОС Windows**

**Проверил:**

Грищенко В.В.

**Выполнил**

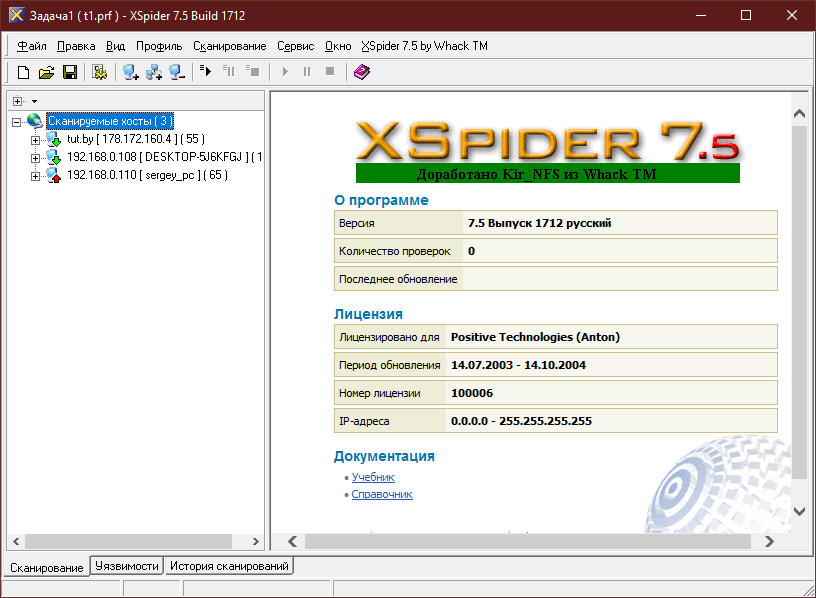
**студент МС-42:**

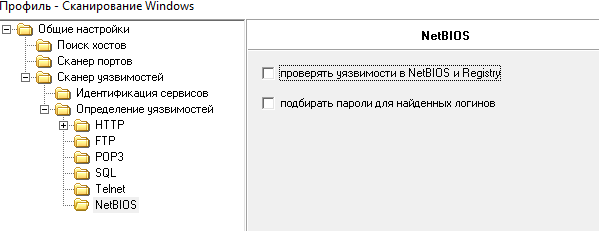
Кузьменцов С.В.

Гомель, 2020

**Последовательность действий**

Шаг 1. Создать профиль «Сканирование Windows». Список портов ограничить значениями 135, 139, 445. В разделе «Сканер UDPсервисов» выбрать «Сканировать UDP-порты» и указать порты служб NTP, Microsoft RPC и NetBIOS Name. Отключить подбор учетных записей. Запустить анализатор протоколов tcpdump или wireshark.





Шаг 2. Создать задачу «Сканирование Windows», указать сервер S2 в качестве объекта сканирования. Выполнить сканирование, проанализировать результаты. Просмотреть трассировку сканирования.

