

Гомельский Государственный Университет
им. Ф. Скорины

**Лабораторная работа №7.
Особенности идентификации уязвимостей ОС
Windows**

Проверил:
Грищенко В.В.

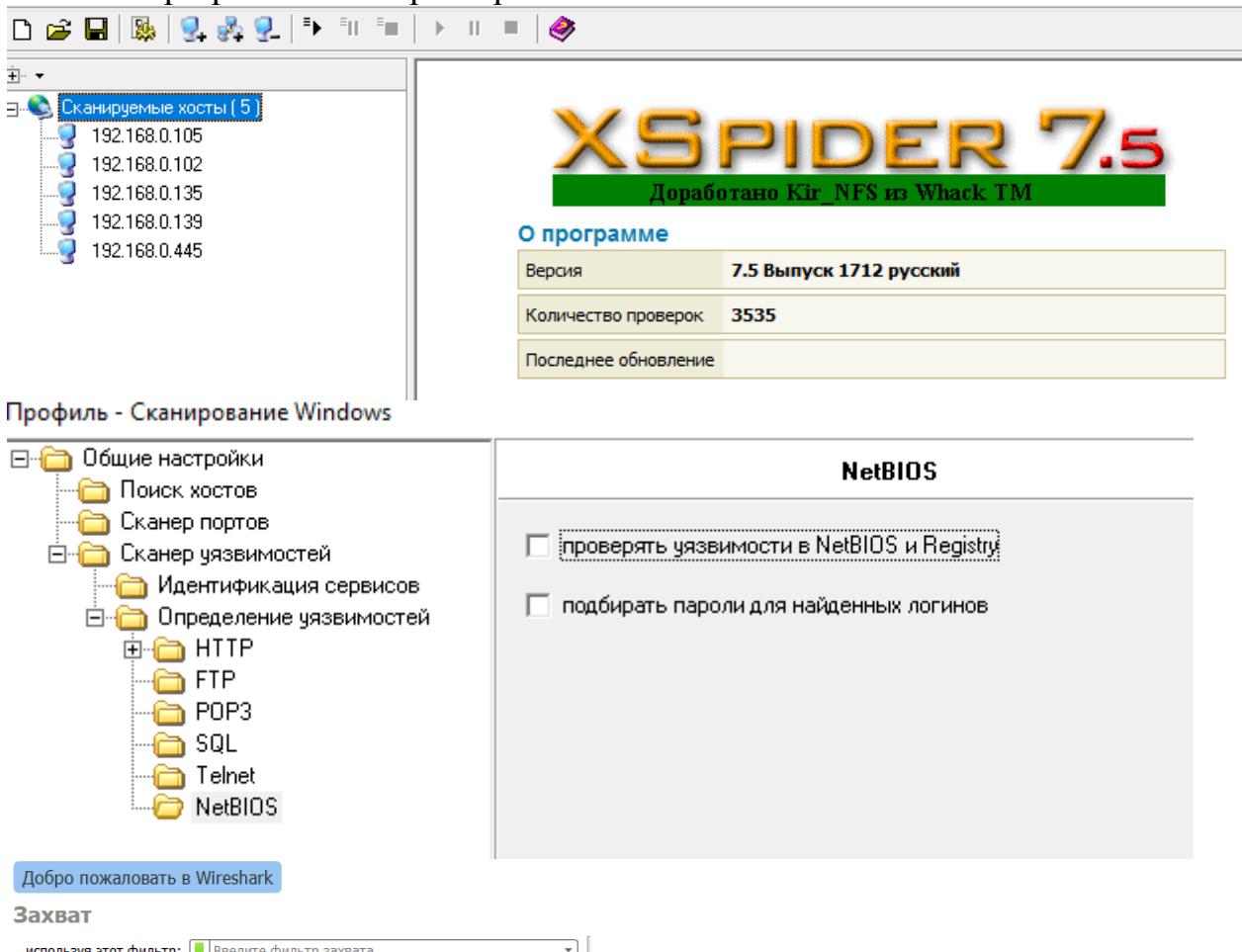
Студент МС – 42:
Кузнецов Ю.В.

г. Гомель

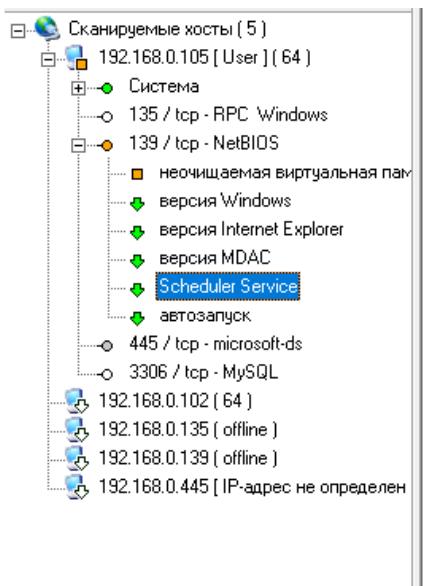
Цель работы: Целью лабораторной работы является обучение основным методам и средствам сканирования уязвимостей ОС Windows.

Постановка задачи: выполнить идентификацию уязвимостей ОС Windows сервера S2 с использованием сканера безопасности XSpider.

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.



⚠ Доступна информация
Scheduler Service

Описание

Если вы не используете планировщик задач, то разумным будет отключить его, т.к. данный сервис часто используется атакующими для запуска вредоносного кода.

Решение

Заблокируйте сервис следующим ключом реестра:
HKEY_LOCAL_MACHINE
SYSTEM\CurrentControlSet\Services\Schedule
Start = 4

