

Гомельский Государственный Университет  
им. Ф. Скорины

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

**Проверил:**

Грищенко В.В.

**Студент МС – 42:**

Кузнецов Ю.В.

**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.

The screenshot displays the XSpider 7.5 application interface. On the left, a tree view shows the scan profile configuration for 'Сканирование Windows'. The 'Сканируемые хосты' (Scannable hosts) list includes five IP addresses: 192.168.0.105, 192.168.0.102, 192.168.0.135, 192.168.0.139, and 192.168.0.445. The 'Профиль - Сканирование Windows' (Profile - Windows Scanning) section is expanded, showing a tree of scan categories: 'Общие настройки' (General settings), 'Поиск хостов' (Host discovery), 'Сканер портов' (Port scanner), 'Сканер уязвимостей' (Vulnerability scanner), 'Идентификация сервисов' (Service identification), and 'Определение уязвимостей' (Vulnerability determination). Under 'Определение уязвимостей', the 'NetBIOS' category is selected. The 'NetBIOS' settings panel on the right shows two unchecked checkboxes: 'проверять уязвимости в NetBIOS и Registry' (check vulnerabilities in NetBIOS and Registry) and 'подбирать пароли для найденных логинов' (select passwords for found logins). Below the settings, a 'Захват' (Capture) section shows a list of network interfaces with their corresponding capture status indicators. The interfaces listed are Ethernet 2, Подключение по локальной сети\* 9, Подключение по локальной сети\* 8, Подключение по локальной сети\* 2, Беспроводная сеть (Wireless network), Подключение по локальной сети\* 10, Adapter for loopback traffic capture, Подключение по локальной сети\* 1, and Ethernet.

О программе	
Версия	7.5 Выпуск 1712 русский
Количество проверок	3535
Последнее обновление	

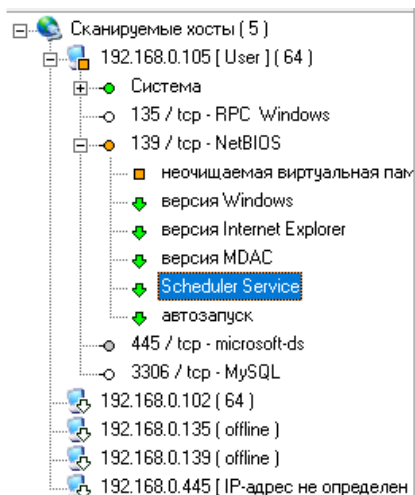
Добро пожаловать в Wireshark

Захват

...используя этот фильтр:

- Ethernet 2
- Подключение по локальной сети\* 9
- Подключение по локальной сети\* 8
- Подключение по локальной сети\* 2
- Беспроводная сеть
- Подключение по локальной сети\* 10
- Adapter for loopback traffic capture
- Подключение по локальной сети\* 1
- Ethernet

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

