Гомельский Государственный Университет им. Ф. Скорины

Лабораторная работа №7. Особенности идентификации уязвимостей ОС Windows

Проверил:

Студент МС – 42:

Грищенко В.В.

Городнянская Анна

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.

±. ▼	NetBIOS
Э Сканируемые хосты (5) 192.168.0.105 192.168.0.135 192.168.0.139 192.168.0.445	проверять уязвимости в NetBIOS и Registry
Добро пожаловать в Wireshark	
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.

