Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №7

«Особенности идентификации уязвимостей ОС Windows»

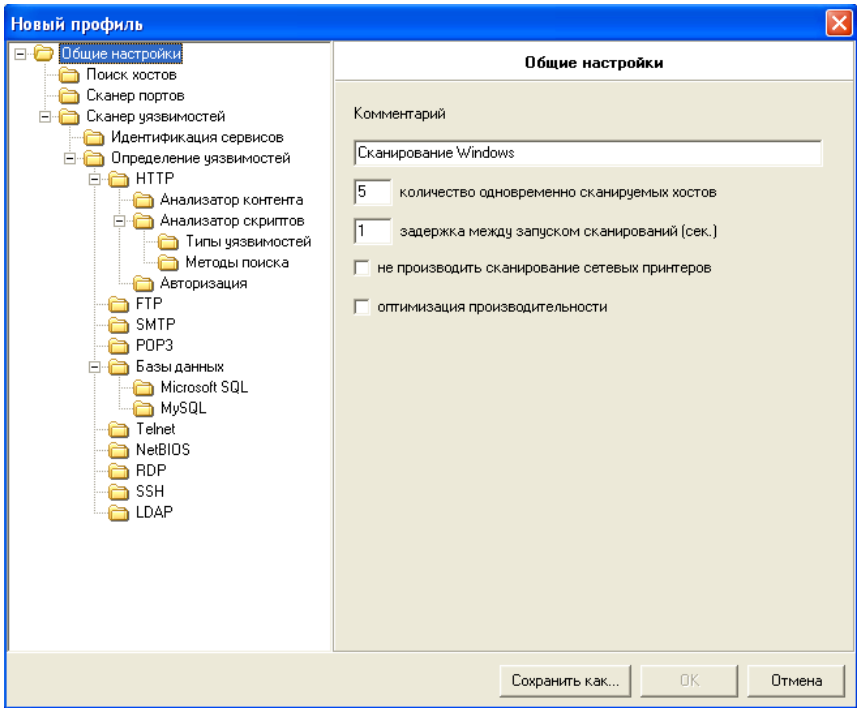
Выполнил:
Студент группы МС-42
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

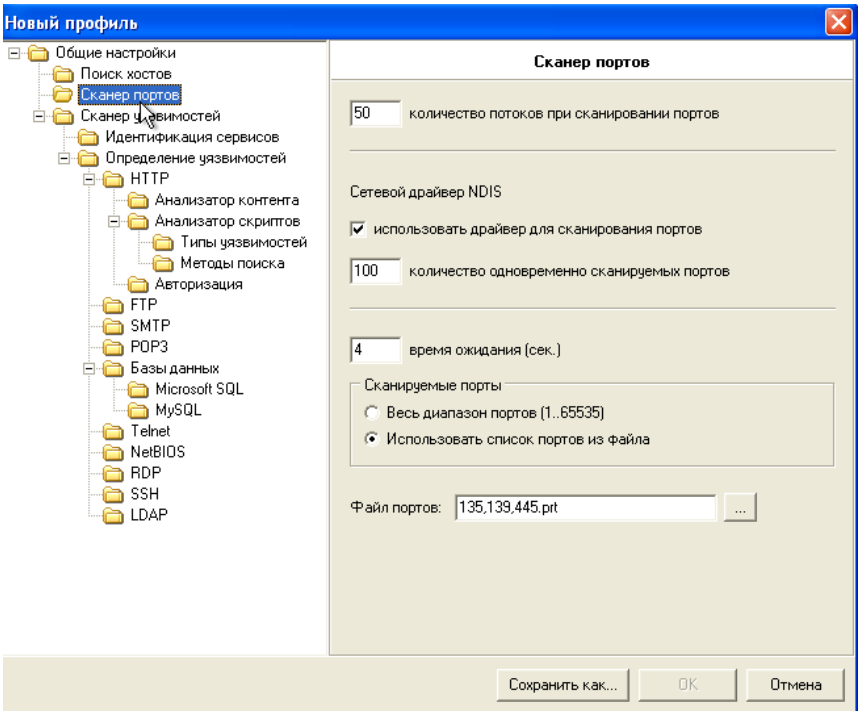
2022

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

Ход работы.

Шаг 1. Создадим профиль «Сканирование Windows». Список портов ограничим значениями 135, 139, 445. В разделе «Сканер UDPсервисов» выберем «Сканировать UDP-порты» и укажем порты служб NTP, Microsoft RPC и NetBIOS Name. Отключим подбор учетных записей.





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

Хост
172.16.0.1

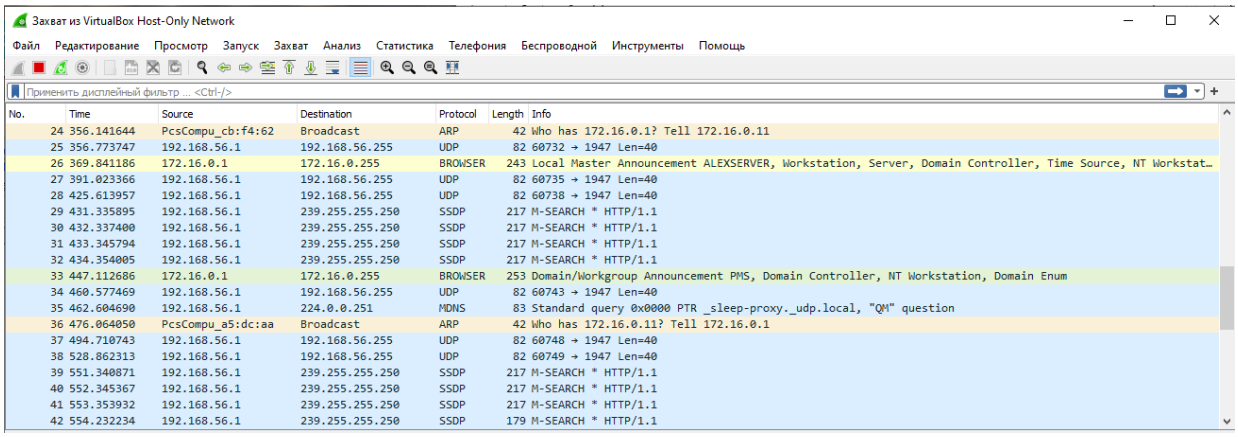
Информация

Имя хоста (полученное при обратном DNS запросе):	**computer.domain**
Время отклика:	**1 мсек**
TTL:	**128**

Параметры сканирования

Начало сканирования:	**07:27:34 07.12.2022**
Время сканирования:	**00:03:53**
Версия:	**7.7 Demo Build 3100**
Профиль:	**Сканирование Windows.prf**

Уязвимость	Хост	Порт	Сервис
Отказ в обслуживании (ms07-058)	172.16.0.1	135 / tcp	Microsoft RPC
Удаленное выполнение кода (ms08-067)	172.16.0.1	445 / tcp	Microsoft DS
рекурсия	172.16.0.1	53 / udp	DNS
список ресурсов	172.16.0.1	139 / tcp	NetBIOS
LanManager и OS	172.16.0.1	139 / tcp	
MAC-адрес	172.16.0.1	139 / tcp	NetBIOS
Windows Server 2003 3790 Service Pack 2	172.16.0.1		
имя компьютера и домен	172.16.0.1	139 / tcp	NetBIOS



Вывод: в ходе лабораторной работы изучили и воспользовались основными методами и средствами сканирования уязвимостей ОС Windows.