

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  
Баль П.М.  
Проверил: Грищенко В.В.

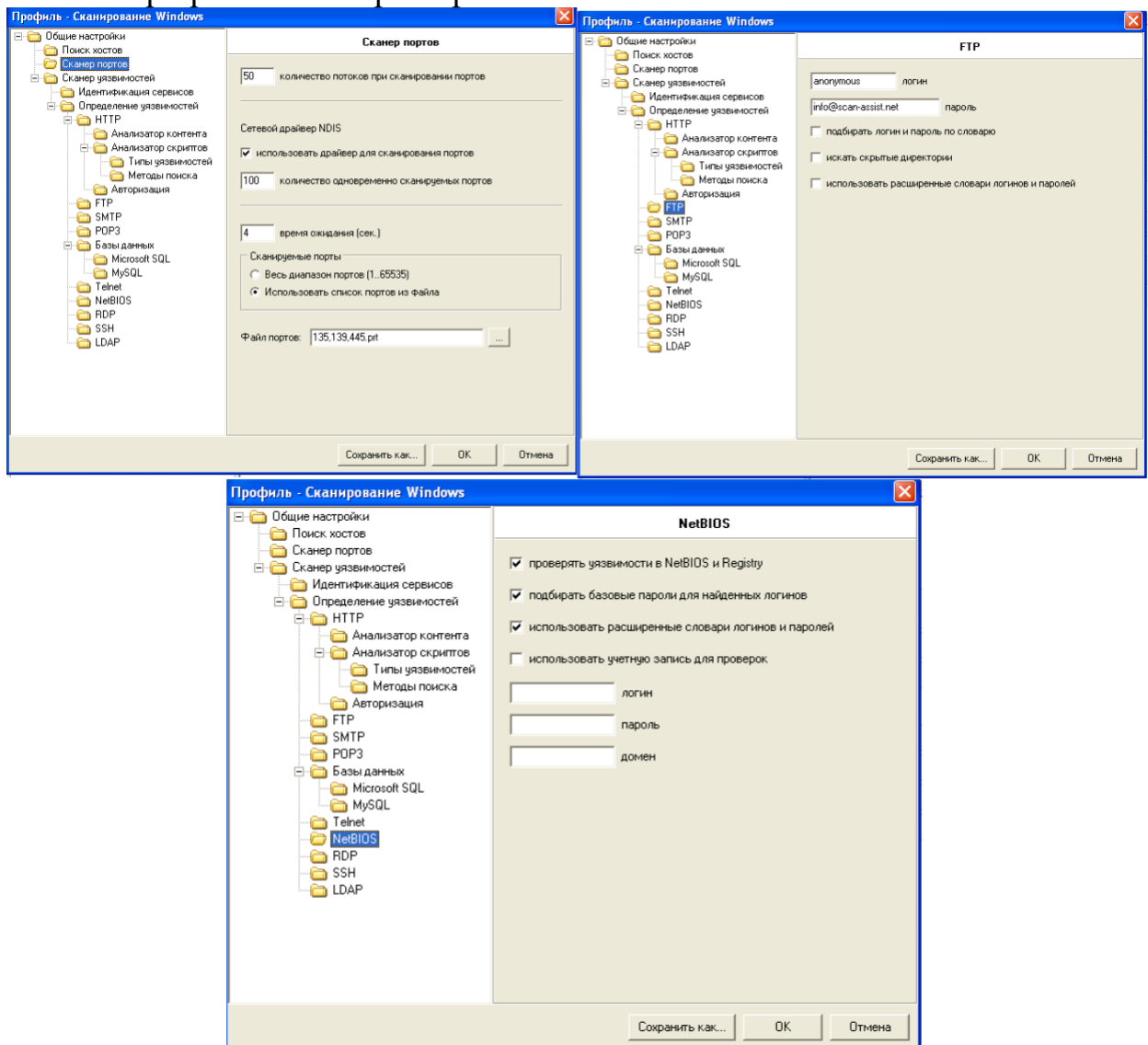
2022

## Лабораторная работа №7

**Цель работы:** 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.

**Сканируемые хосты { 1 }**

- 172.16.0.1 [ computer.domain ] [ 128 ]
  - Система
    - Windows Server 2003 3790 Servi
  - 53 / udp - DNS
    - Рекурсия
  - 123 / udp - NTP
  - 135 / tcp - Microsoft RPC
    - Отказ в обслуживании (ms07-058)
  - 137 / udp - NetBIOS Name
  - 139 / tcp - NetBIOS
    - Список ресурсов
    - LanManager и OS
    - MAC-адрес
    - Имя компьютера и домен
  - 445 / tcp - Microsoft DS
    - Удаленное выполнение кода (ms08-067)

**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:	21:24:38 03.12.2022
Версия:	7.7 Demo Build 3100
Профиль:	Сканирование Windows.prf

**Задача3 ( Сканирование Windows.prf ) - XSpider 7.7 Demo Build 3100**

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	NetBIOS
MAC-адрес	172.16.0.1	139 / tcp	NetBIOS
Windows Server 2003 3790 Service Pack 2	172.16.0.1	139 / tcp	NetBIOS
имя компьютера и домен	172.16.0.1	139 / tcp	NetBIOS

**Описание уязвимости**

имя компьютера и домен

Доступна информация  
**Имя компьютера и домен**

**Описание**

Имя компьютера : ALEXSERVER  
Домен : PMS

**Список пакетов**

No.	Time	Source	Destination	Protocol	Length	Info
5	23.042380553	PcsCompu_b1:21:7c	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.8
14	165.129073087	172.16.0.1	172.16.0.255	BROWSER	243	Local Master Announcement ALEXSERVER, Workstation, Server, Do
19	237.473336681	172.16.0.8	172.16.0.255	BROWSER	243	Host Announcement ALEX1, Workstation, Server, NT Workstation
24	248.709147802	172.16.0.1	172.16.0.255	BROWSER	253	Domain/Workgroup Announcement PMS, Domain Controller, NT Work
45	577.913863442	172.16.0.7	172.16.0.255	NBNS	92	Name query NB DESKTOP-74M2B7G<1c>
46	578.663908744	172.16.0.7	172.16.0.255	NBNS	92	Name query NB DESKTOP-74M2B7G<1c>
47	579.414558112	172.16.0.7	172.16.0.255	NBNS	92	Name query NB DESKTOP-74M2B7G<1c>

**Frame 14: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface eth0, id 0**

Ethernet II, Src: PcsCompu\_52:64:3a (08:00:27:52:64:3a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

SMB (Server Message Block Protocol)

SMB Mailslot Protocol

**Microsoft Windows Browser Protocol**

Command: Local Master Announcement (0x0f)

Update Count: 0

Update Periodicity: 12 minutes

Host Name: ALEXSERVER

Windows version: Windows Server 2003 R2 or Windows Server 2003

OS Major Version: 5

OS Minor Version: 2

Server Type: 0x0084102b, Workstation, Server, Domain Controller, Time Source, NT Workstation, Master Browser, DFS

Browser Protocol Major Version: 15

Browser Protocol Minor Version: 1

Signature: 0xaa55

Host Comment:

**Вывод:** в ходе лабораторной работы были изучены методы и средства сканирования уязвимостей ОС Windows, выполнена идентификация уязвимостей ОС Windows сервера S2 с использованием сканера безопасности XSpider.