

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
Созинов Л.В.
Проверил:
Грищенко В.В.

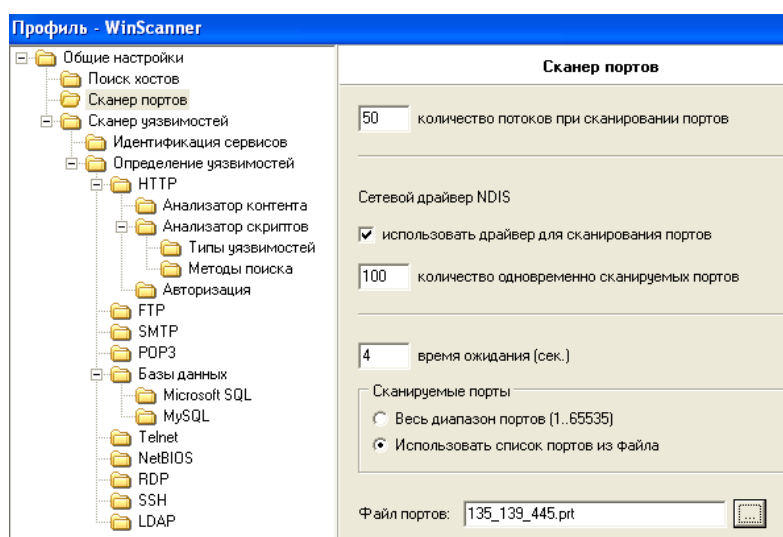
Лабораторная работа №7

Особенности идентификации уязвимостей ОС Windows

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

Ход работы

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.



2. Создать задачу «Сканирование Windows», указать сервер S2 в качестве объекта сканирования. Выполнить сканирование, проанализировать результаты. 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:	11:57:49 07.12.2022
Время сканирования:	00:03:47
Версия:	7.7 Demo Build 3100
Профиль:	WinScanner.prf

Задача1 (WinScanner.prf) - XSpider 7.7 Demo Build 3100			
Файл Правка Вид Профиль Сканирование Сервис Окно Справка			
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	172.16.0.11	139 / tcp	
LanManager и OS	172.16.0.1	139 / tcp	
MAC-адрес	172.16.0.1	139 / tcp	NetBIOS
Windows 5.1	172.16.0.11		
Windows Server 2003 3790 Service Pack 2	172.16.0.1		
имя компьютера и домен	172.16.0.1	139 / tcp	NetBIOS

No.	Time	Source	Destination	Protocol	Length	Info
24	356.141644	PcsCompu_cb:f4:62	Broadcast	ARP	42	Who has 172.16.0.1? Tell 172.16.0.11
25	356.773747	192.168.56.1	192.168.56.255	UDP	82	60732 → 1947 Len=40
26	369.841186	172.16.0.1	172.16.0.255	BROWSER	243	Local Master Announcement ALEXSERVER, Workstation, Server, Domain Controller, Time
27	391.823365	192.168.56.1	192.168.56.255	UDP	82	60735 → 1947 Len=40
28	425.613957	192.168.56.1	192.168.56.255	UDP	82	60738 → 1947 Len=40
29	431.335895	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
30	432.337400	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
31	433.345704	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
32	434.354805	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
33	447.112686	172.16.0.1	172.16.0.255	BROWSER	253	Domain/Workgroup Announcement PMS, Domain Controller, NT Workstation, Domain Enum
34	460.577469	192.168.56.1	192.168.56.255	UDP	82	60743 → 1947 Len=40
35	462.604690	192.168.56.1	224.0.0.251	MDNS	83	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question
36	476.064050	PcsCompu_a5:dc:aa	Broadcast	ARP	42	Who has 172.16.0.11? Tell 172.16.0.1
37	494.718743	192.168.56.1	192.168.56.255	UDP	82	60746 → 1947 Len=40
38	528.862313	192.168.56.1	192.168.56.255	UDP	82	60749 → 1947 Len=40
39	551.340871	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
40	552.345367	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
41	553.353932	192.168.56.1	239.255.255.250	SSDP	217	N-SEARCH * HTTP/1.1
42	554.232234	192.168.56.1	239.255.255.250	SSDP	179	N-SEARCH * HTTP/1.1