

Министерство образования Республики Беларусь

Учреждение образования

«Гомельский государственный университет

имени Франциска Скорины»

Отчёт по лабораторной работе №7

«Особенности идентификации уязвимостей ОС Windows»

Выполнил студент группы МС-42:

Казак И.В.

Проверил:

Старший преподаватель

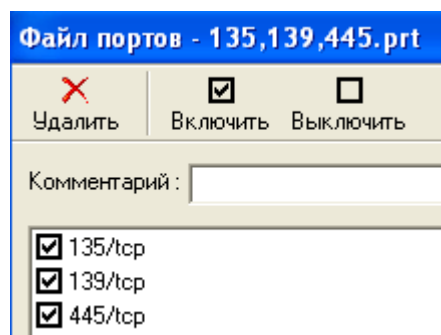
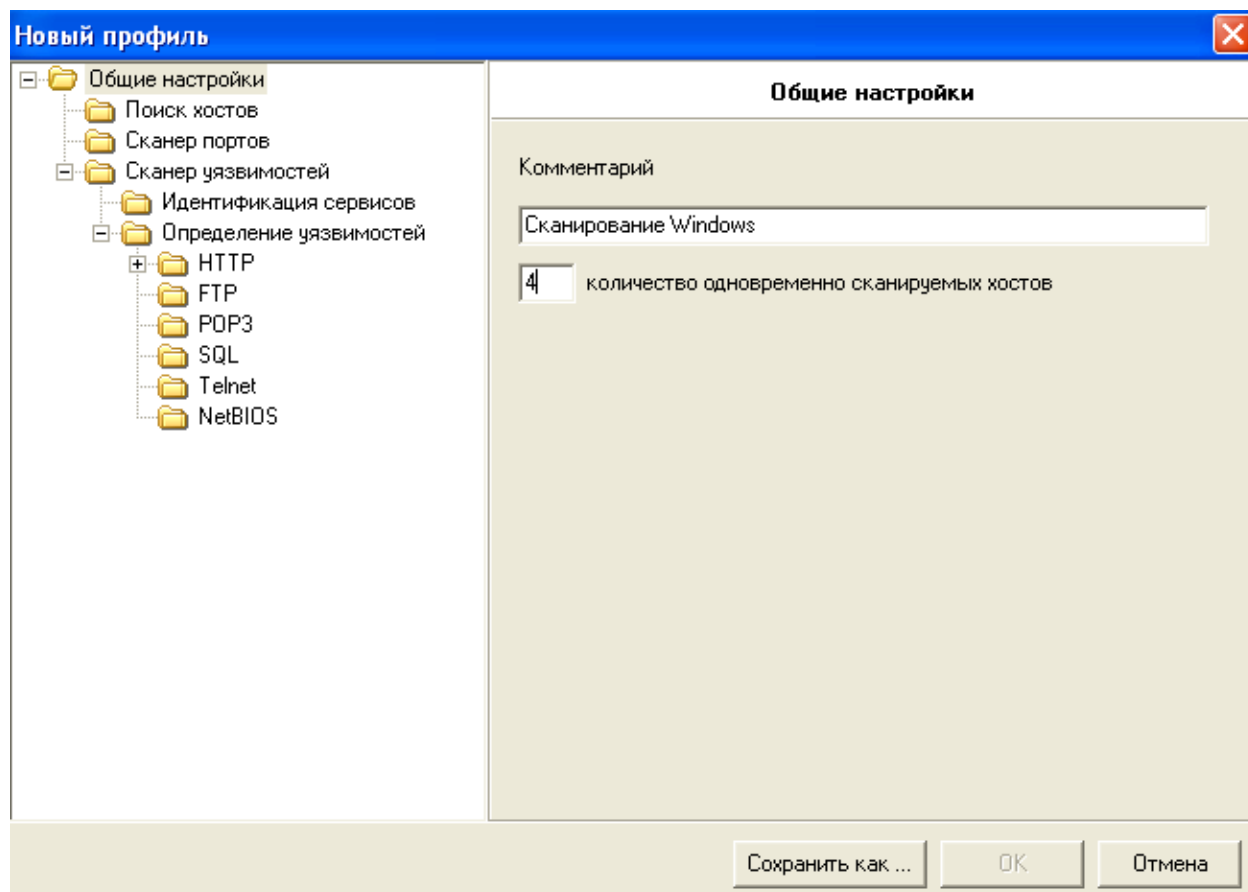
Грищенко В.В.

Гомель 2022

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

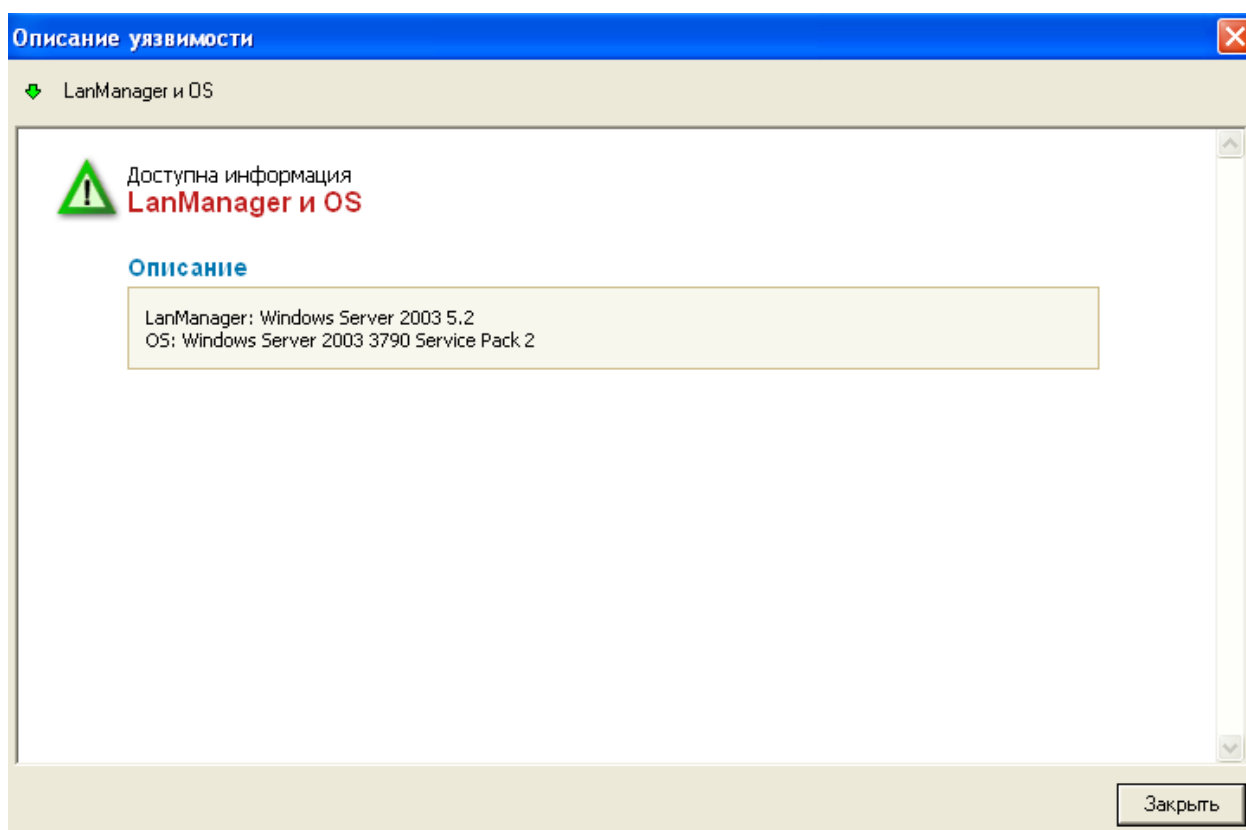
Ход работы.

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. Запустить анализатор протоколов tcpdump или wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_9f:62:4d	Broadcast	ARP	42	who has 172.16.0.1? Tell 172.16.0.20
2	18.866054	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3	19.867898	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	20.875439	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	21.883120	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	66.842389	172.16.0.20	172.16.0.255	BROWSER	249	Host Announcement USER1, Workstation, Server, NT Workstation, Potential Browser, Backup Browser
7	77.026812	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8	78.035570	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
9	79.042851	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10	80.050689	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
11	138.872517	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	139.873961	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13	140.874854	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
14	141.883340	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
15	178.379342	fe80::a00:27ff:fef6_	ff02::2	ICMPv6	62	Router Solicitation
16	197.035818	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
17	198.042601	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18	199.050322	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	200.052282	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	258.880889	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21	259.883317	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22	260.891862	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

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



Описание уязвимости

Windows Server 2003 3790 Service Pack 2

!

Доступна информация

Windows Server 2003 3790 Service Pack 2

Описание

Вероятная версия операционной системы : Windows Server 2003 3790 Service Pack 2

Закреть

Захват из Беспроводная сеть

Файл

Редактирование

Просмотр

Запуск

Захват

Анализ

Статистика

Телефония

Беспроводной

Инструменты

Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
66	7.352357	SamsungE_bd:52:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
67	7.659917	192.168.1.36	192.168.1.255	NBNS	92	Name query NB WPAD<00>
68	7.695890	192.168.1.7	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
69	7.793912	192.168.1.5	192.168.1.7	SSDP	324	HTTP/1.1 200 OK
70	7.899567	192.168.1.2	192.168.1.7	UDP	419	41555 → 64780 Len=377
71	7.980291	192.168.1.2	224.0.0.7	UDP	213	8001 → 8001 Len=171
72	8.480653	fe80::25d0:a1ee:67b...	ff02::1:3	LLMNR	84	Standard query 0x9643 A wpad
73	8.505830	192.168.1.36	224.0.0.252	LLMNR	64	Standard query 0x9643 A wpad
74	8.581307	fe80::25d0:a1ee:67b...	ff02::1:3	LLMNR	84	Standard query 0x9643 A wpad
75	8.581307	192.168.1.36	224.0.0.252	LLMNR	64	Standard query 0x9643 A wpad
76	8.703854	192.168.1.7	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
77	8.790963	192.168.1.36	192.168.1.255	NBNS	92	Name query NB WPAD<00>
78	8.792201	192.168.1.2	192.168.1.7	UDP	419	47506 → 64780 Len=377
79	8.798400	192.168.1.5	192.168.1.7	SSDP	324	HTTP/1.1 200 OK
80	9.392426	SamsungE_bd:52:57	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
81	9.507415	192.168.1.36	192.168.1.255	NBNS	92	Name query NB WPAD<00>
82	9.710910	192.168.1.7	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
83	9.837527	192.168.1.5	192.168.1.7	SSDP	324	HTTP/1.1 200 OK
84	9.922294	192.168.1.2	192.168.1.7	UDP	419	57837 → 64780 Len=377
85	10.027045	192.168.1.2	224.0.0.7	UDP	213	8001 → 8001 Len=171
86	10.121825	192.168.1.2	192.168.1.255	UDP	77	52896 → 15600 Len=35
87	10.224703	192.168.1.36	192.168.1.255	NBNS	92	Name query NB WPAD<00>

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

tcp

No.	Time	Source	Destination	Protocol	Length	Info
31	3.794609	192.168.1.7	20.54.24.246	TCP	66	58792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32	3.891492	20.54.24.246	192.168.1.7	TCP	66	443 → 58792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=256 SACK_PERM
33	3.891552	192.168.1.7	20.54.24.246	TCP	54	58792 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
34	3.891929	192.168.1.7	20.54.24.246	TLSv1.2	276	Client Hello
35	3.967406	20.54.24.246	192.168.1.7	TCP	1414	443 → 58792 [ACK] Seq=1 Ack=223 Win=524544 Len=1360 [TCP segment of a reassembled PDU]
36	3.967406	20.54.24.246	192.168.1.7	TLSv1.2	1126	Server Hello, Certificate, Server Key Exchange, Server Hello Done
37	3.967455	192.168.1.7	20.54.24.246	TCP	54	58792 → 443 [ACK] Seq=223 Ack=2433 Win=66560 Len=0
38	3.970508	192.168.1.7	20.54.24.246	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
40	4.043911	20.54.24.246	192.168.1.7	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
41	4.043911	20.54.24.246	192.168.1.7	TLSv1.2	123	Application Data
42	4.044003	192.168.1.7	20.54.24.246	TCP	54	58792 → 443 [ACK] Seq=381 Ack=2553 Win=66304 Len=0
43	4.045051	192.168.1.7	20.54.24.246	TLSv1.2	141	Application Data
44	4.045177	192.168.1.7	20.54.24.246	TLSv1.2	92	Application Data
45	4.045260	192.168.1.7	20.54.24.246	TLSv1.2	203	Application Data
46	4.045376	192.168.1.7	20.54.24.246	TLSv1.2	737	Application Data
48	4.118489	20.54.24.246	192.168.1.7	TLSv1.2	92	Application Data
49	4.120153	20.54.24.246	192.168.1.7	TCP	54	443 → 58792 [ACK] Seq=2591 Ack=655 Win=524288 Len=0
50	4.154261	20.54.24.246	192.168.1.7	TLSv1.2	96	Application Data
51	4.154261	20.54.24.246	192.168.1.7	TLSv1.2	522	Application Data
52	4.154416	192.168.1.7	20.54.24.246	TCP	54	58792 → 443 [ACK] Seq=1338 Ack=3101 Win=65792 Len=0
96	14.236203	192.168.1.7	40.79.141.152	TCP	55	58745 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
97	14.320378	40.79.141.152	192.168.1.7	TCP	66	443 → 58745 [ACK] Seq=1 Ack=2 Win=2047 Len=0 SLE=1 SRE=2

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