Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Отчёт по лабораторной работе №7
«Особенности идентификации уязвимостей ОС Windows»

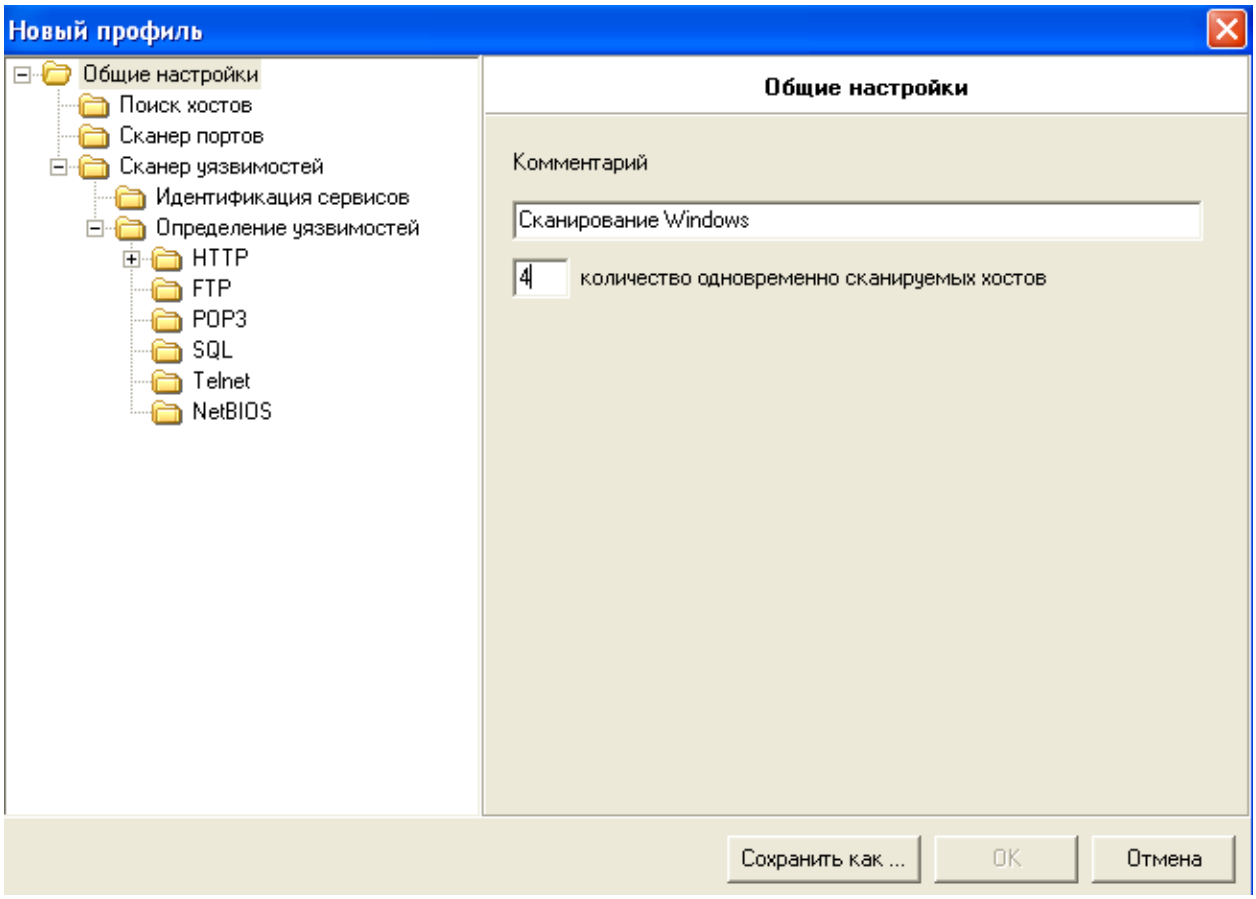
Выполнил студент группы МС-42: Казак И.В.
Проверил:
Старший преподаватель Грищенко В.В.

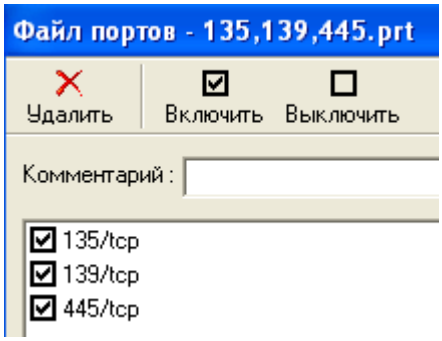
Гомель 2022

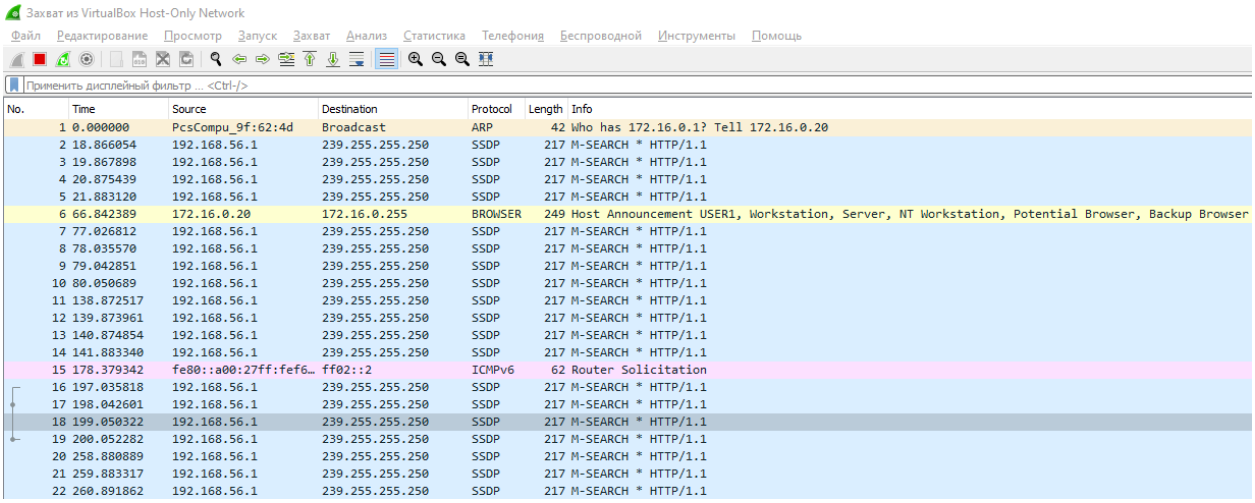
Цель работы: обучение основным методам и средствам сканирования уязвимостей ОС Windows.

Ход работы.

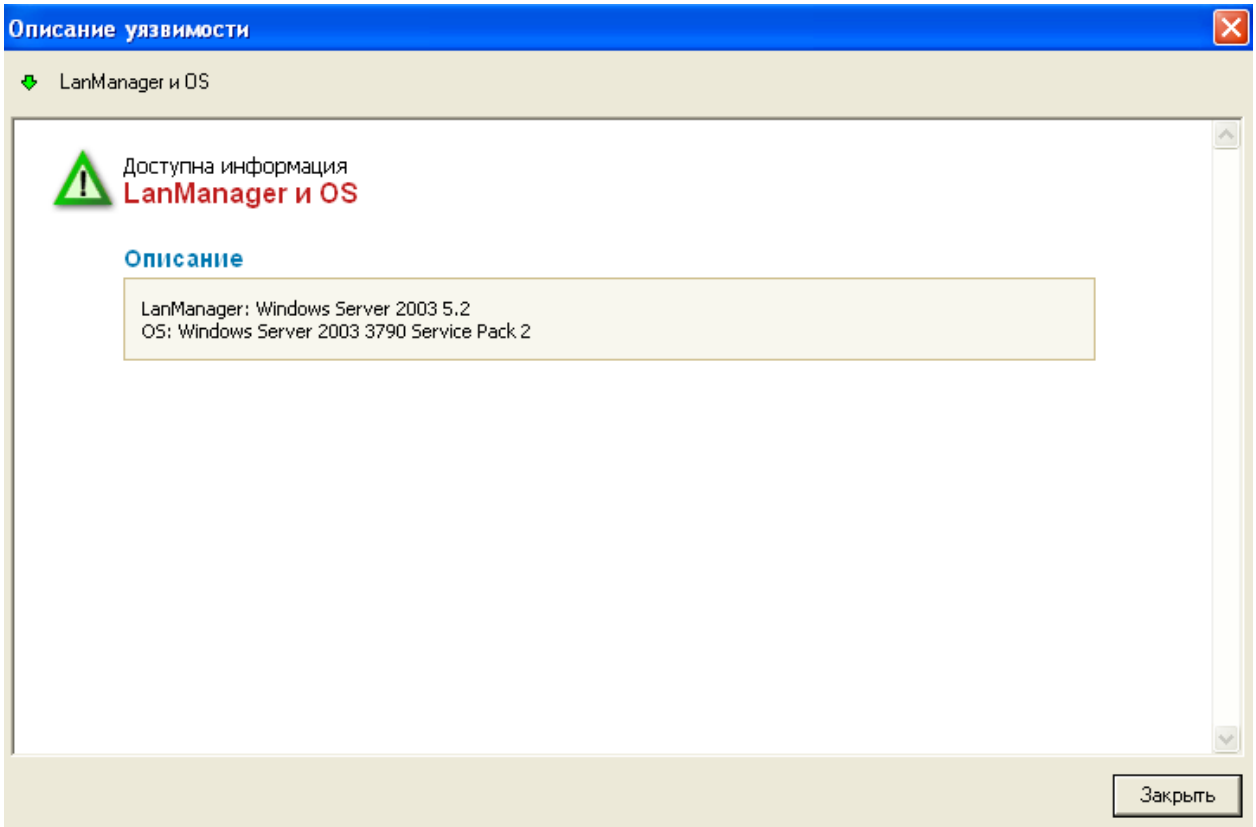
Шаг 1. Создадим профиль «Сканирование Windows». Список портов ограничим значениями 135, 139, 445. В разделе «Сканер UDPсервисов» выберем «Сканировать UDP-порты» и укажем порты служб NTP, Microsoft RPC и NetBIOS Name. Отключим подбор учетных записей. Запустить анализатор протоколов tcpdump или wireshark.

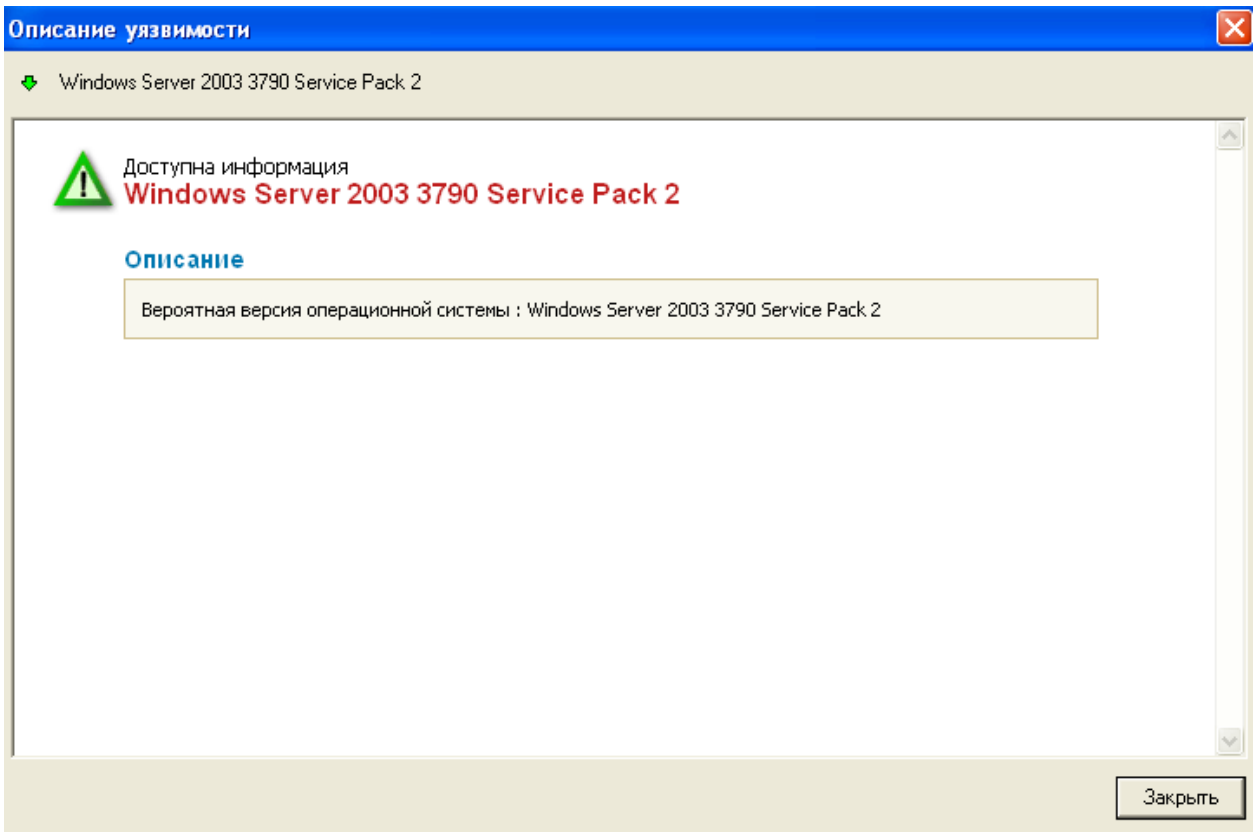





Захват из VirtualBox Host-Only Network
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
Применить дисплейный фильтр ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 PcsCompu_9f:62:4d Broadcast ARP 42 Who has 172.16.0.1? Tell 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.



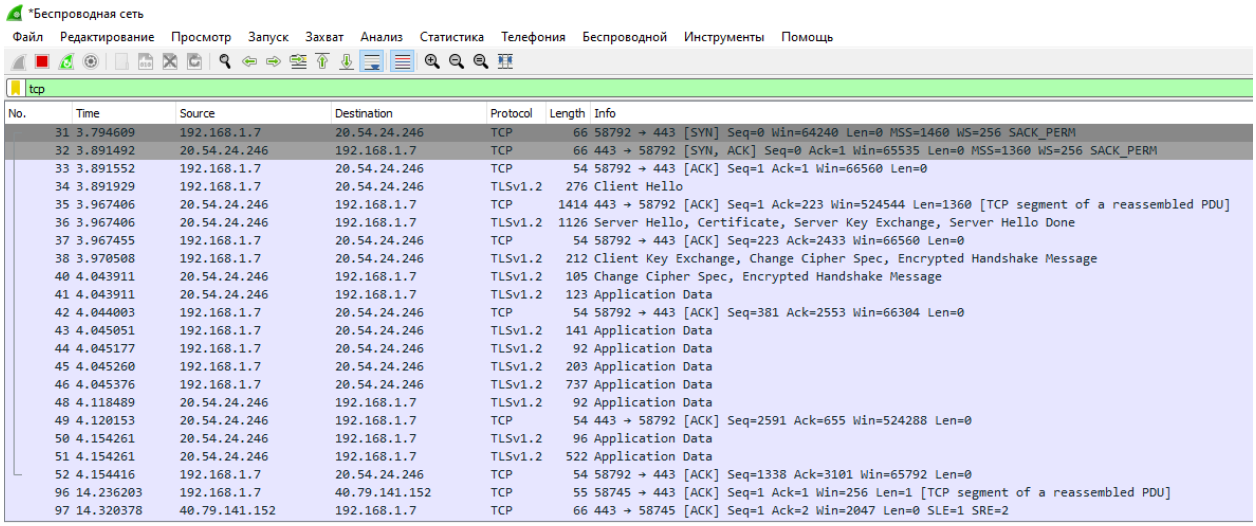


Захват из Беспроводная сеть

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>



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