

УО «Гомельский государственный университет им. Ф. Скорины»
Физический факультет
Кафедра общей физики

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7

Особенности идентификации уязвимостей ОС Windows

Проверил:
Грищенко В.В.

Выполнили:
студент группы МС-42
Гончаров Владислав

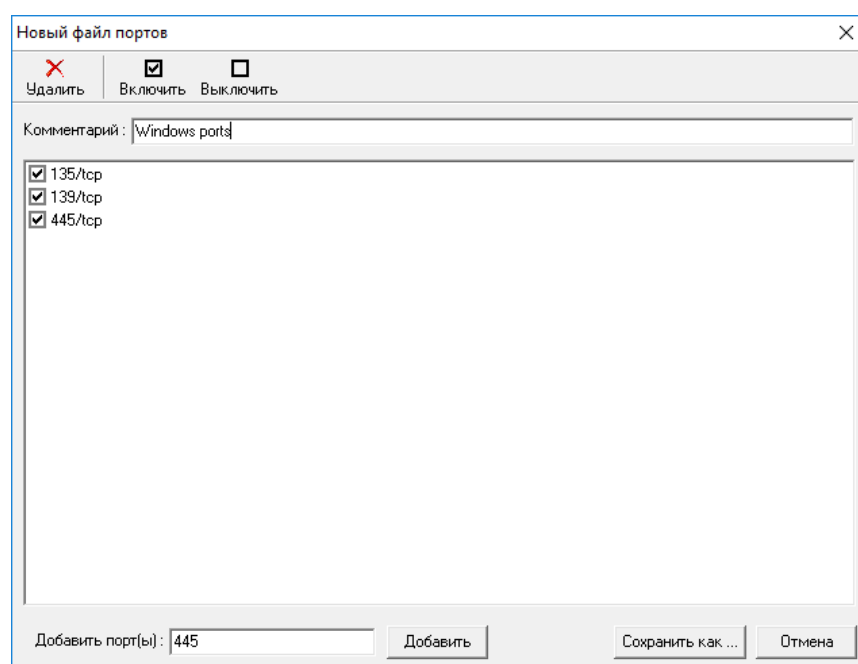
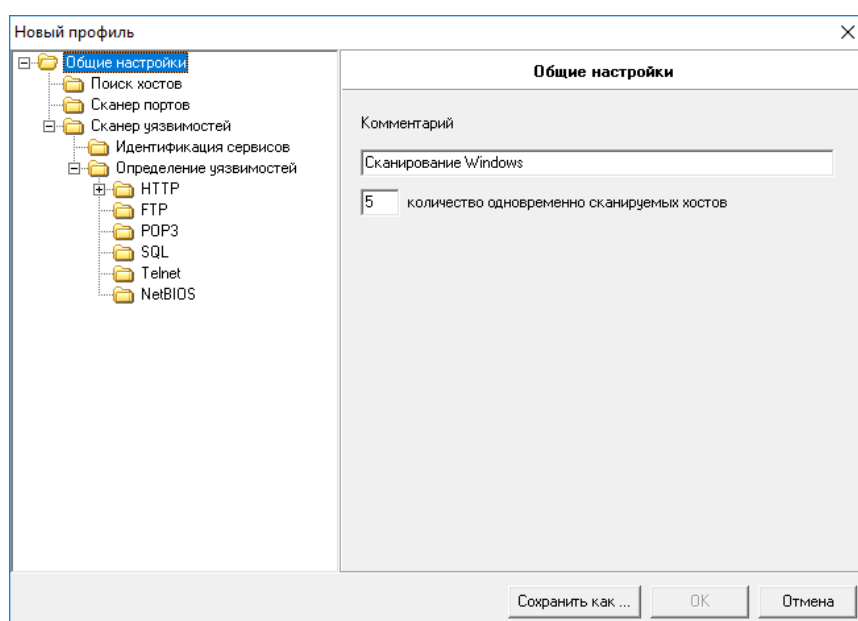
Гомель 2020

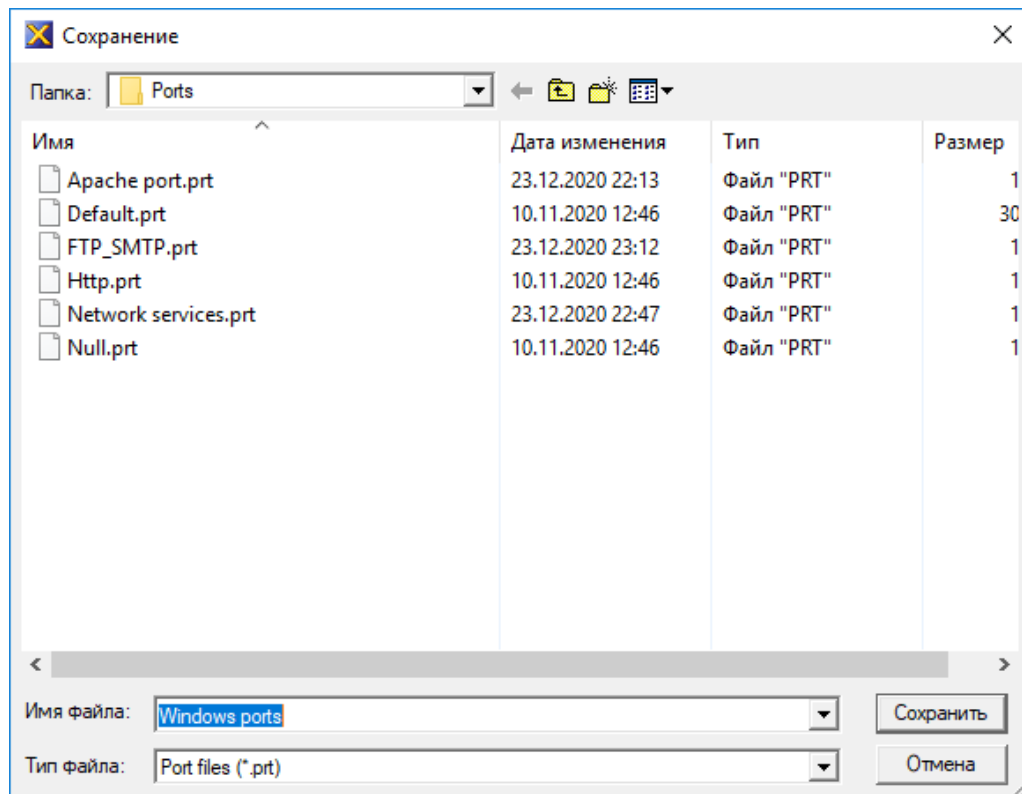
Лабораторная работа №7

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

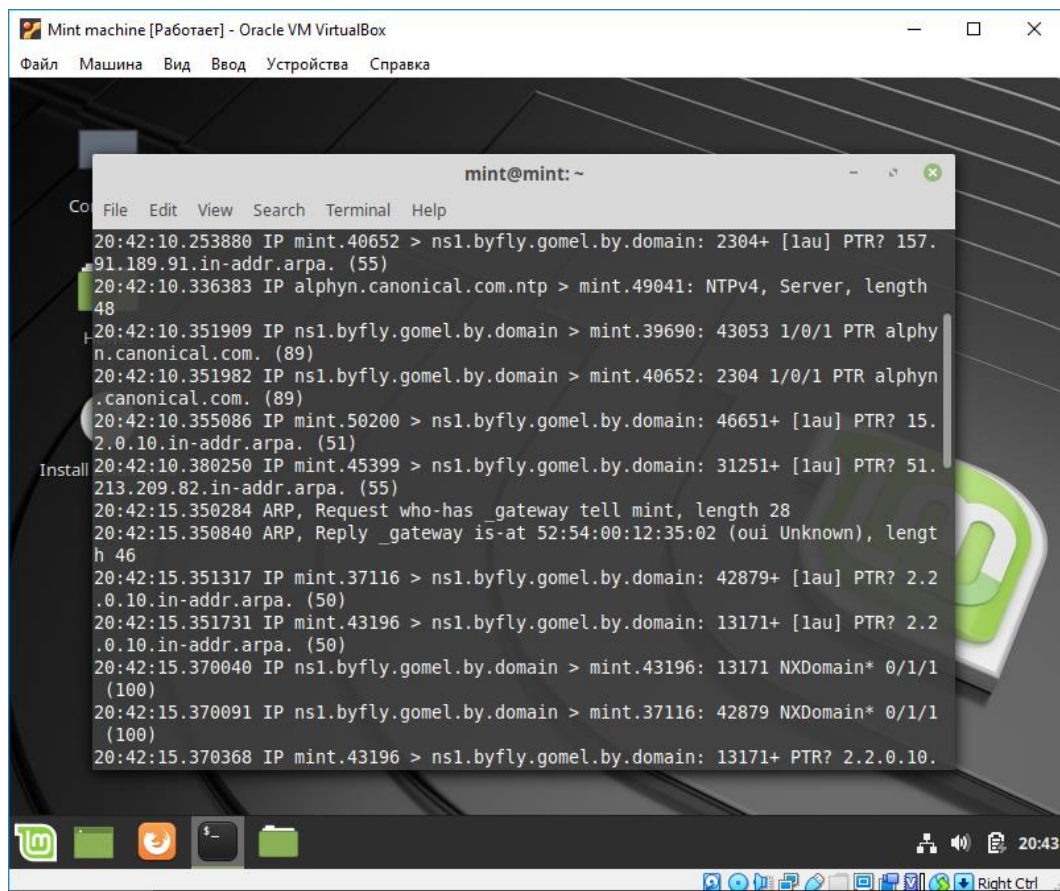
Постановка задачи: выполнить идентификацию уязвимостей ОС Windows сервера с использованием сканера безопасности XSpider.

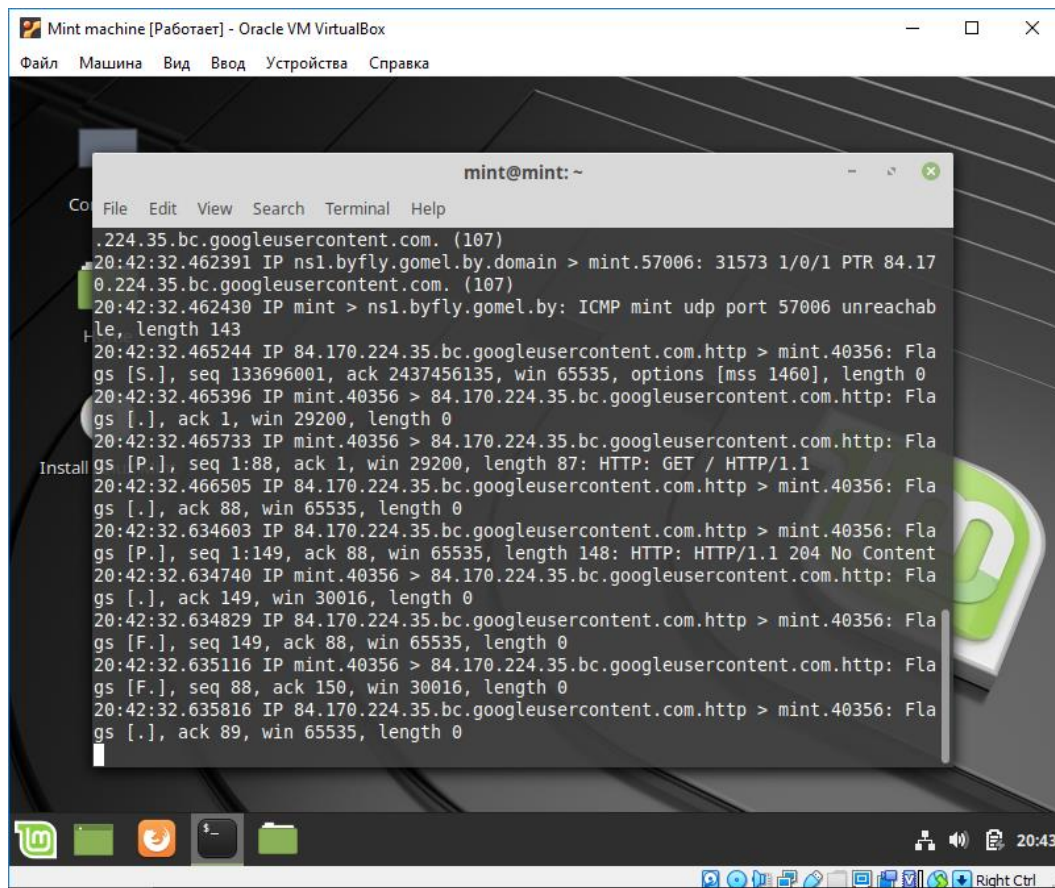
Шаг 1. Создать профиль «Сканирование Windows». Список портов ограничить значениями 135, 139, 445. В разделе «Сканер UDPсервисов» выбрать «Сканировать UDP-порты» и указать порты служб NTP, Microsoft RPC и NetBIOS Name. Отключить подбор учетных записей.



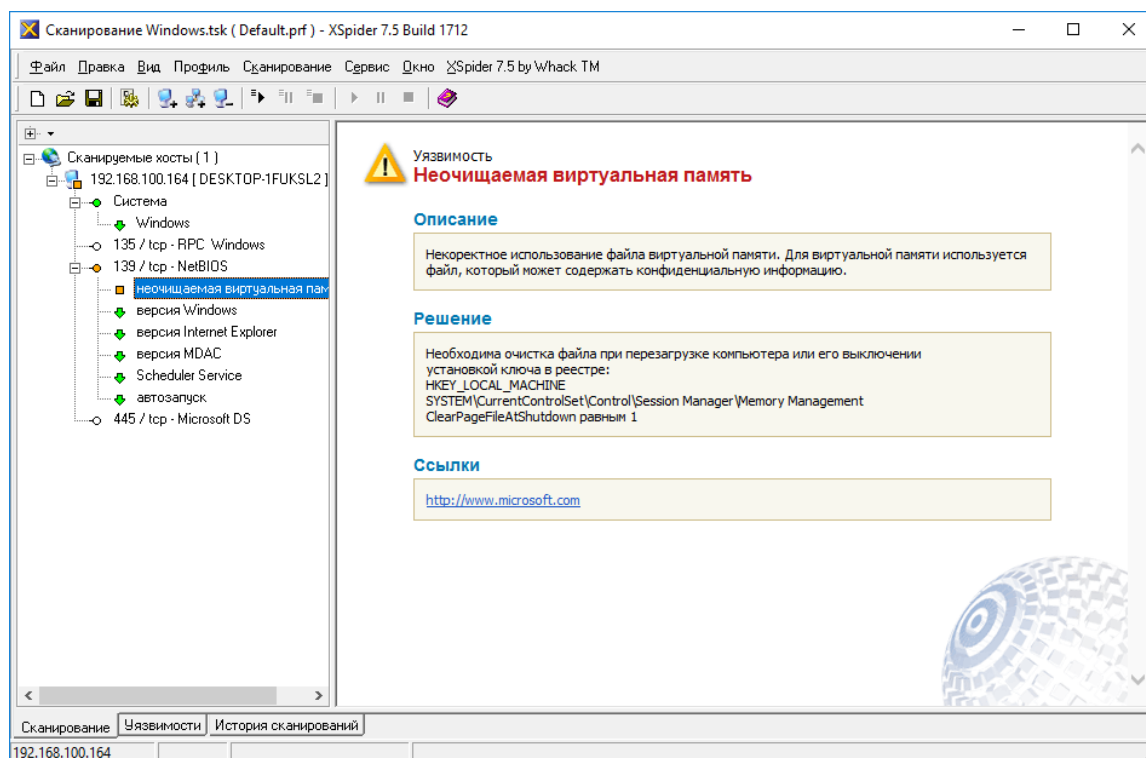


Шаг 2. Запустить анализатор протоколов tcpdump или wireshark.





Шаг 3. Создать задачу «Сканирование Windows», указать сервер S2 в качестве объекта сканирования. Выполнить сканирование, проанализировать результаты. Просмотреть трассировку сканирования.



| Уязвимость | | | | | Хост | Порт | Сервис | |
|----------------------------------|--|--|--|--|-----------------|-----------|---------|--|
| ■ неочищаемая виртуальная память | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |
| ◆ Scheduler Service | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |
| ◆ Windows | | | | | 192.168.100.164 | | | |
| ◆ автозапуск | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |
| ◆ версия Internet Explorer | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |
| ◆ версия MDAC | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |
| ◆ версия Windows | | | | | 192.168.100.164 | 139 / tcp | NetBIOS | |