Министерство образования Республики Беларусь Учреждение образования

“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №4

«Идентификация операционных систем»

2022

Выполнил: Студент группы МС-42

Рыбалкин Д.С.

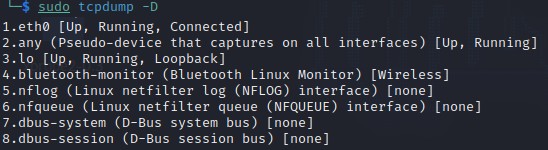
Проверил: Грищенко В.В.

**Лабораторная работа №4**

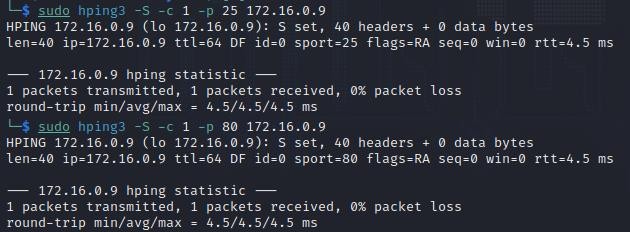
***Цель работы:*** обучение современным методам и средствам идентификации ОС анализируемой КС.

**Постановка задачи:** выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

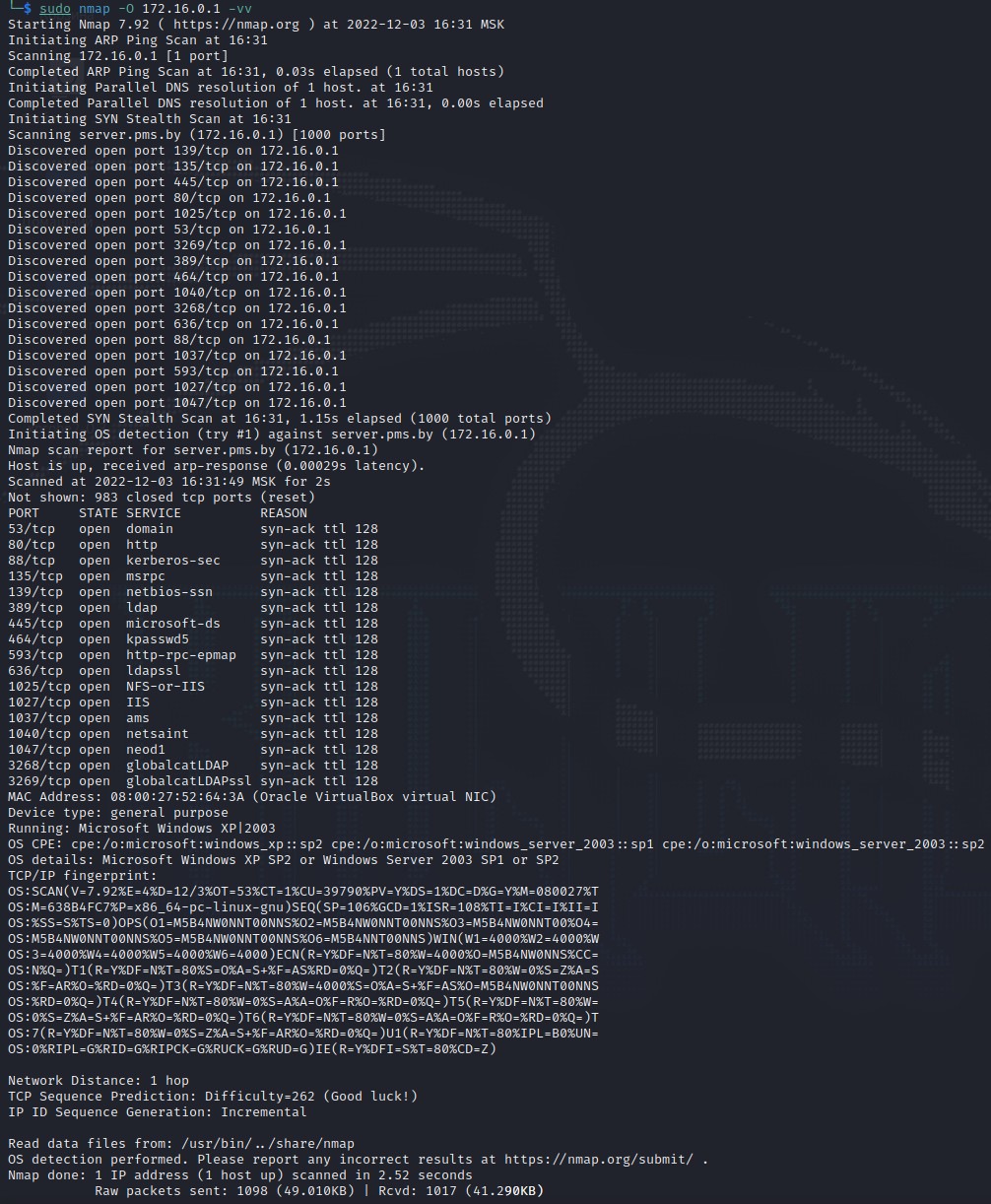
**Шаг 1.** Загрузить виртуальную машину TWS1. Войти в систему. Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.



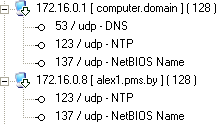
**Шаг 2.** С помощью утилиты hping2 исследовать значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно:



**Шаг 3.** С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

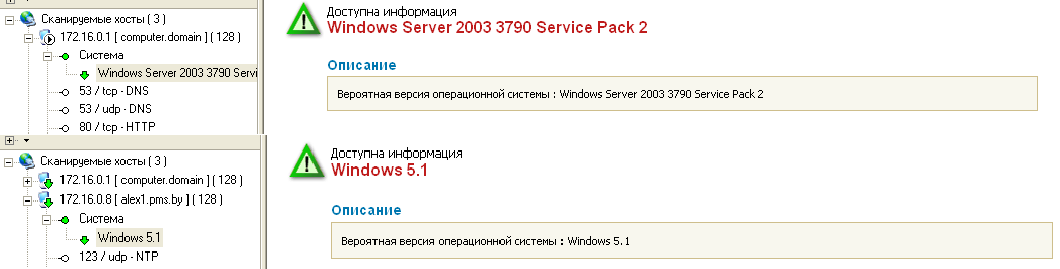


**Шаг 4.** На узле TWS2 перейти в консоль XSpider. Обратить внимание на результаты определения ОС в ходе предыдущих сканирований. В используемом профиле сократить диапазон портов до 1–30 и выполнить повторное сканирование. Убедиться, что ОС не определена.



**Шаг 5.** В профили сканирования включить опции «Искать уязвимости»,

«Искать скрытые каталоги». Выполнить сканирование. убедиться в том, что ОС идентифицирована.



**Вывод:** в ходе лабораторной работы были изучены современные методы и средства идентификации ОС анализируемой КС, выполнена идентификация ОС узлов сети и анализ возможностей сетевых сканеров.