Гомельский Государственный Университет

им. Ф. Скорины

**Лабораторная работа №4.**

**Идентификация операционных систем**

**Проверил: Студент МС – 42:**

Грищенко В.В. Туманский Э.С.

г. Гомель

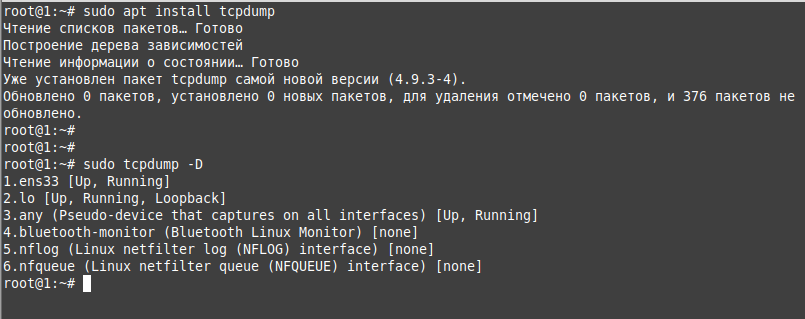
**Цель работы:** Целью лабораторной работы является обучение современным методам и средствам идентификации ОС анализируемой КС.

**Постановка задачи**

Выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

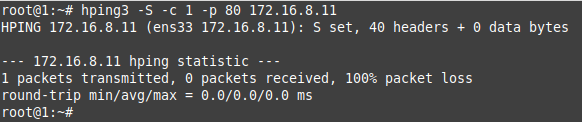
**Последовательность действий**

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



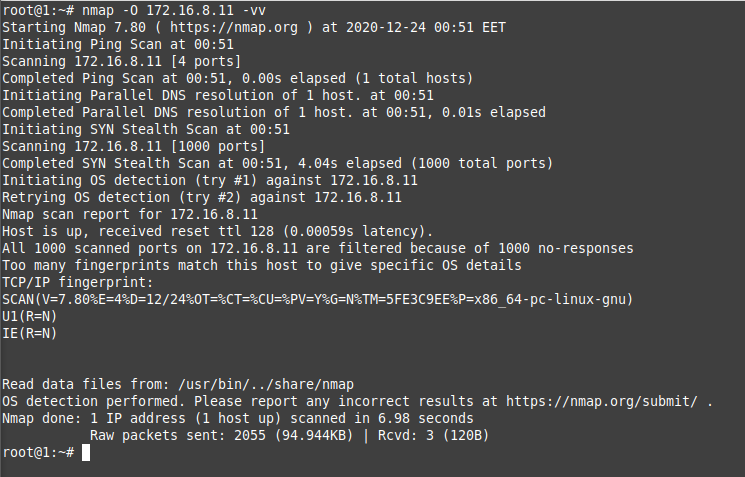
**Шаг 2.** С помощью утилиты hping2 исследовать значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно:

**hping3 –S –c 1 –p 80 172.16.8.11**

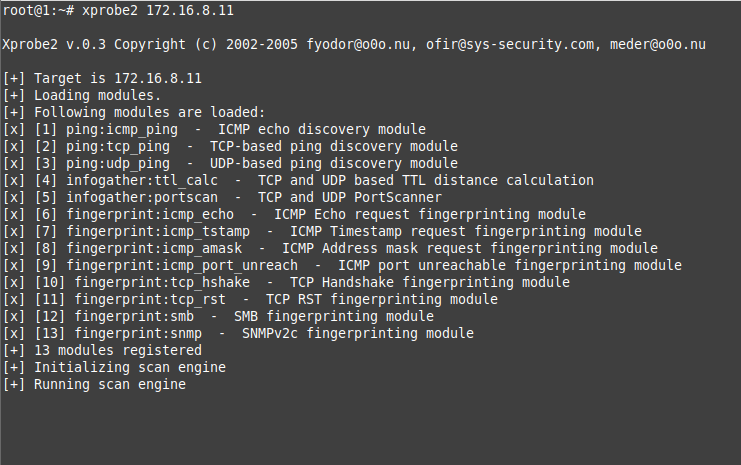


**Шаг 3.** С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

**nmap –O 172.16.8.11 –vv**



**Шаг 4.** С помощью сетевого сканера xprobe выполнить идентификацию ОС с использованием опроса модуля ICMP:

**xprobe2 172.16.8.11** 

**Шаг 5.** 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.

В профили сканирования включить опции «Искать уязвимости»,

«Искать скрытые каталоги». Выполнить сканирование. Убедиться в том, что

ОС идентифицирована.

