Гомельский Государственный Университет

им. Ф. Скорины

**Лабораторная работа №2.**

**Идентификация узлов и портов сетевых служб**

**Проверил: Студент МС – 42:**

Грищенко В.В. Лыч А.Ю.

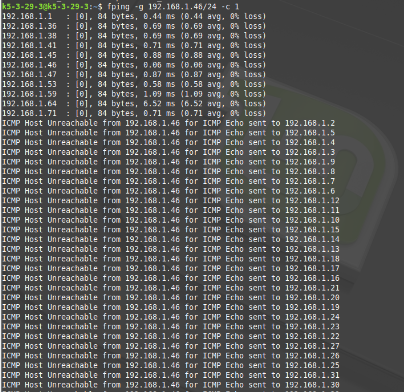
г. Гомель

**Цель работы:** Целью лабораторной работы является обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

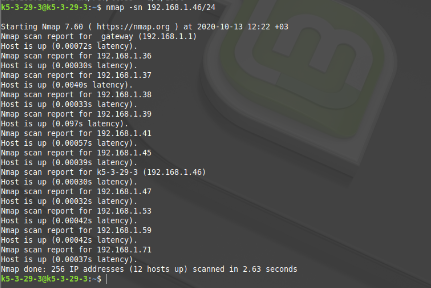
**Постановка задачи:** выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

**Последовательность действий**

**Шаг 1**. Выполнить идентификацию узлов с помощью средства fping для сети 192.168.1.0/24. Просмотреть трассировку сканирования: **fping –g 192.168.1.46/24 –c 1**

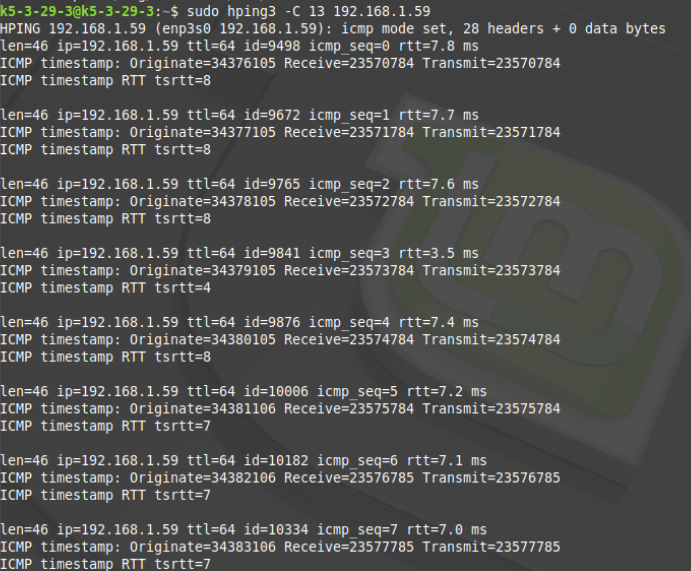


**Шаг 2.** С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования: **nmap –sn 192.168.1.46/24**



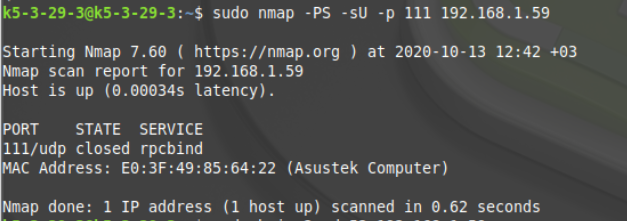
**Шаг 3.** С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request.

Например: **hping3 –C 13 192.168.1.59** Просмотреть трассировку сканирования.



**Шаг 4.** С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.

Например: **nmap –PS –sU –p 111 192.168.1.59**



**Шаг 5.** На узле TWS1 с помощью сетевого сканера nmap выполнить идентификацию открытых TCP и UDP портов найденных узлов IP-сети 172.16.8.0/24, используя основные методы сканирования.

Например: **nmap –sS –n 192.168.1.59,**

**nmap –sS –n 192.168.1.37,**

**nmap –sS –n 192.168.1.41**

Просмотреть трассировки сканирований. Проанализировать результаты.

