Гомельский Государственный Университет

им. Ф. Скорины

**Лабораторная работа №2.**

**Идентификация узлов и портов сетевых служб**

**Проверил: Студент МС – 42:**

Грищенко В.В. Туманский Э.С.

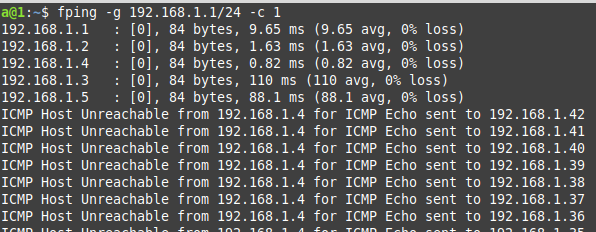
г. Гомель

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

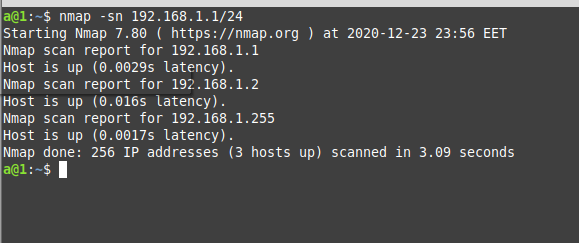
**Постановка задачи:** Выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

**Последовательность действий**

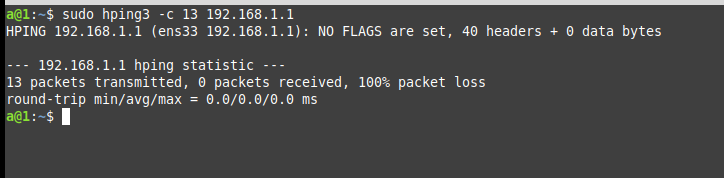
Шаг 1. Выполнить идентификацию узлов с помощью средства fping для сети 192.168.1.1/24. Просмотреть трассировку сканирования: fping –g 192.168.1.1/24 –c 1



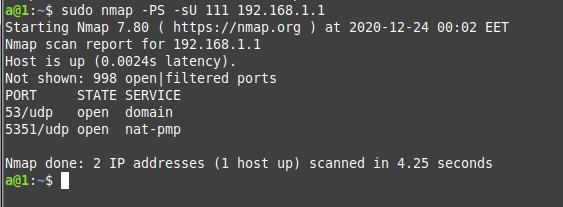
Шаг 3. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования: nmap –sn 192.168.1.1/24



Шаг 4. С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request.



Шаг 5. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.



Шаг 6. На узле TWS1 с помощью сетевого сканера nmap выполнить идентификацию открытых TCP и UDP портов найденных узлов IP-сети 192.168.1.1/24, используя основные методы сканирования.

