**Гомельский государственный университет**

**имени Франциска Скорины**

**Лабораторная работа №2.**

**Идентификация узлов и портов сетевых служб**

**Выполнил Назаров Д. В.**

**Проверил Грищенко В. В.**

**г. Гомель 2020**

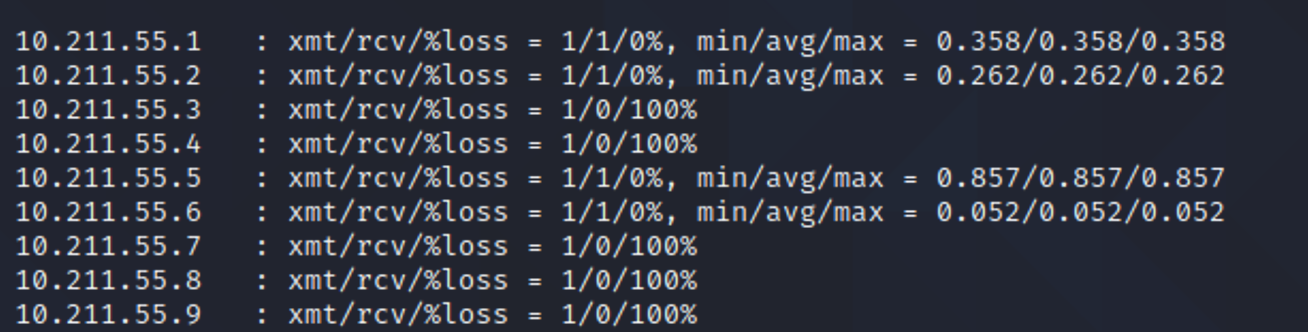
**Цель работы:** Целью лабораторной работы является обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

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

**Последовательность действий**

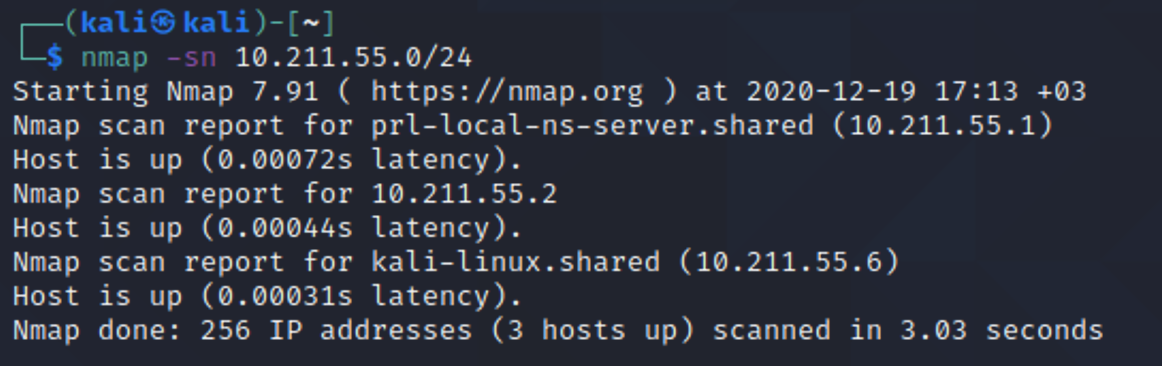
Шаг 2. Выполнить идентификацию узлов с помощью средства fping для сети **10.211.55.0/24**. Просмотреть трассировку сканирования:

**fping –g 10.211.55.0/24 –c 1**



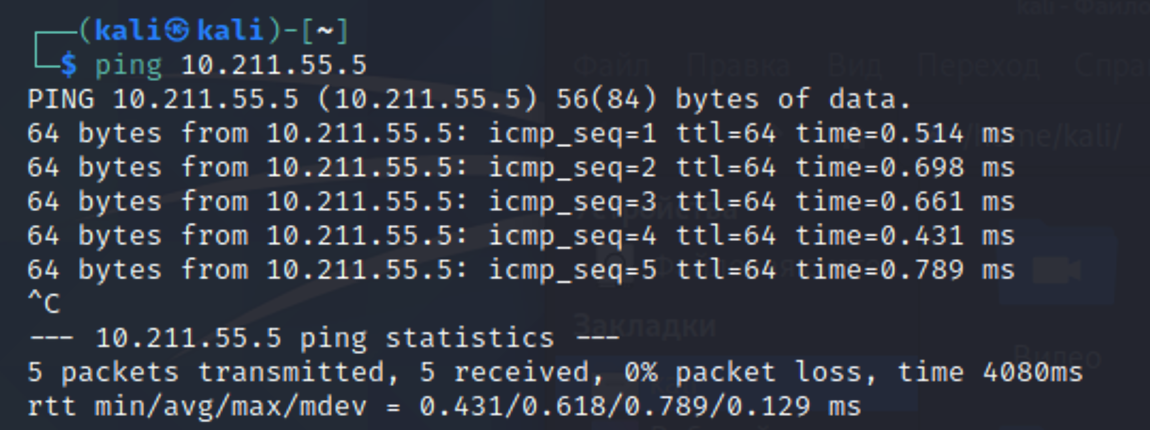
Шаг 3. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования:

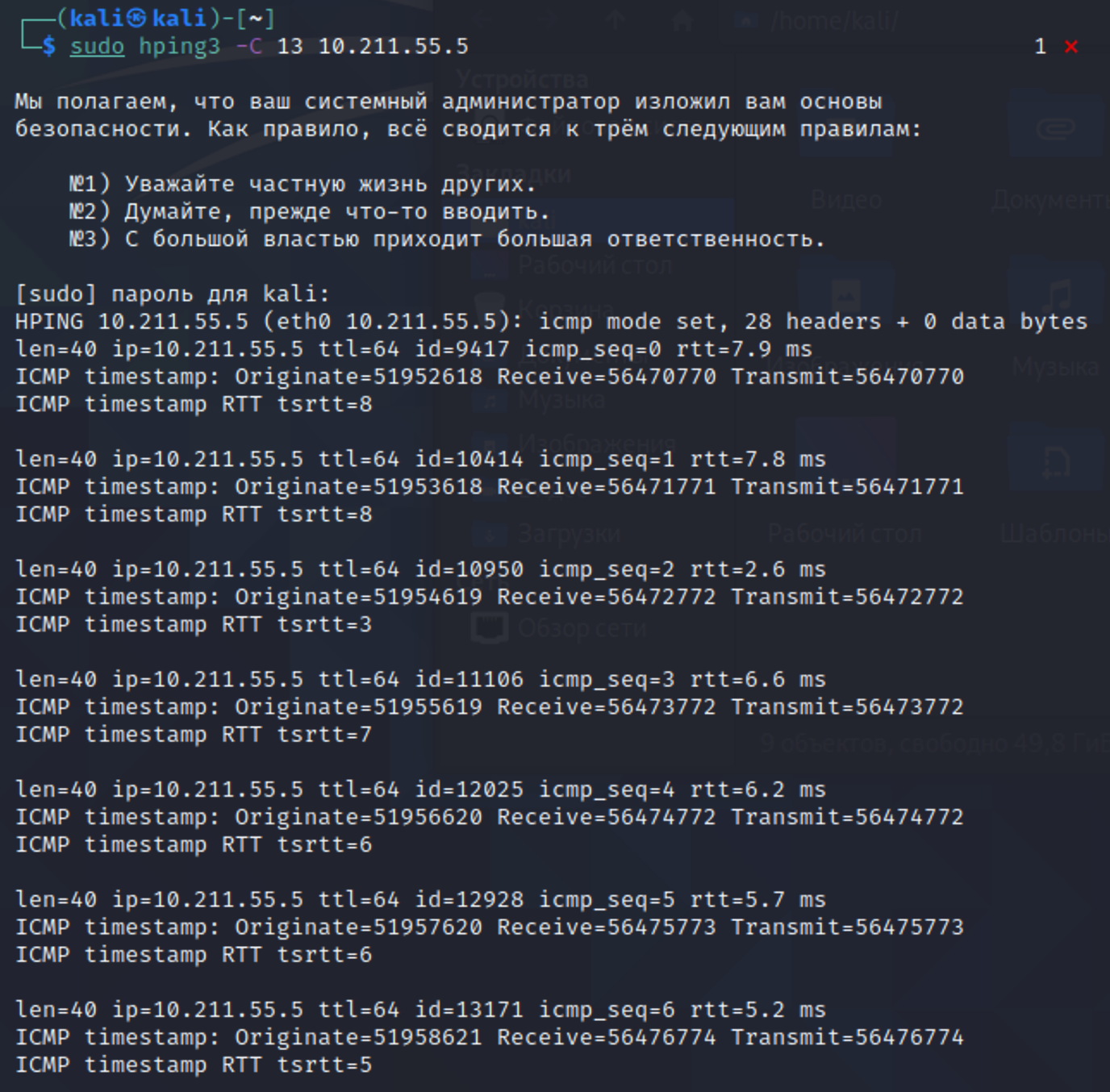
**nmap –sn 192.168.1.46/24**



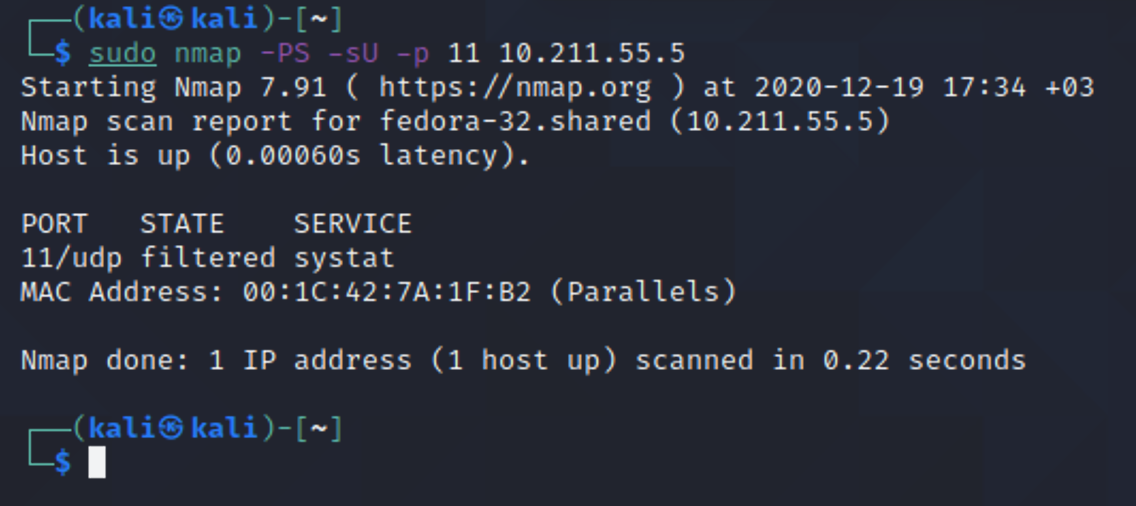
Шаг 4. С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request, Address Mask Request.

В сети развернута только одна машина, кроме Kali



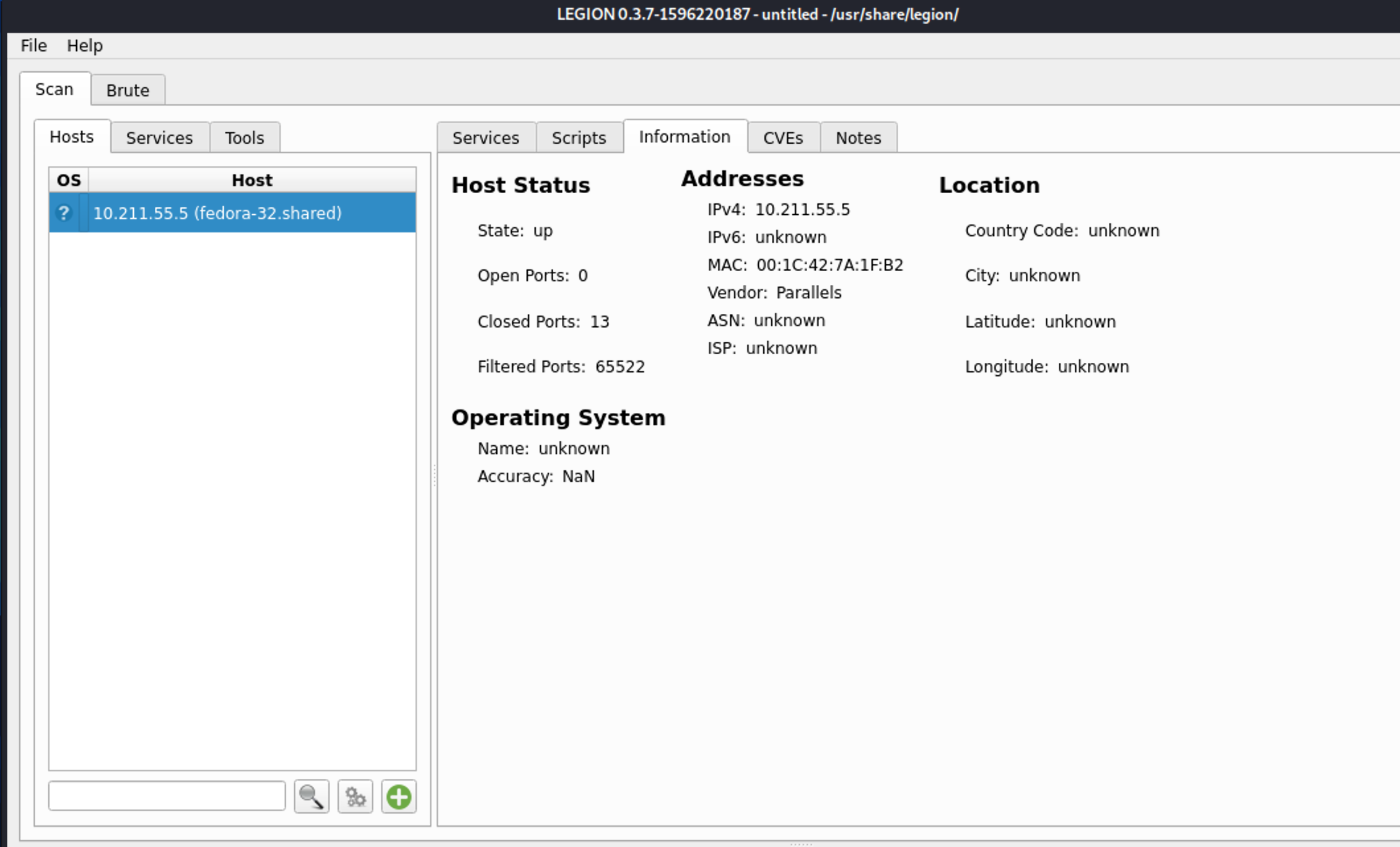


Шаг 5. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.



Шаг 6. На узле TWS2 запустить сканер безопасности XSpider. Создать новый профиль, выбрав параметры ICMP ping и TCP ping, в секции «Сканер UDP сервисов» отключить опцию «Сканировать UDP порты», в секции «Сканер уязвимостей» отключить опцию «Искать уязвимости». Указать диапазон IP-адресов. Выполнить сканирование сети.

Так как xspider коммерческая разработка, используем Legion. Legion не дает одновременно сканировать udp и tcp, при tcp сканировании выпадает ошибка. При запуске персонализированного сканирования сканирование бесконечно. При выборе easy и aggressive mode мы получаем данную информацию



Шаг 7. На узле TWS1 с помощью сетевого сканера nmap выполнить идентификацию открытых TCP и UDP портов найденных узлов IP-сети, используя основные методы сканирования.

**Nmap -sS 11 10.211.55.5**

