Затем переходим к настройкам Linux-Kali. После загрузки проверим настройки: открываем терминал (1), запрашиваем настройки интерфейса (2) и видим на входном интерфейсе (3) адрес остутвует.

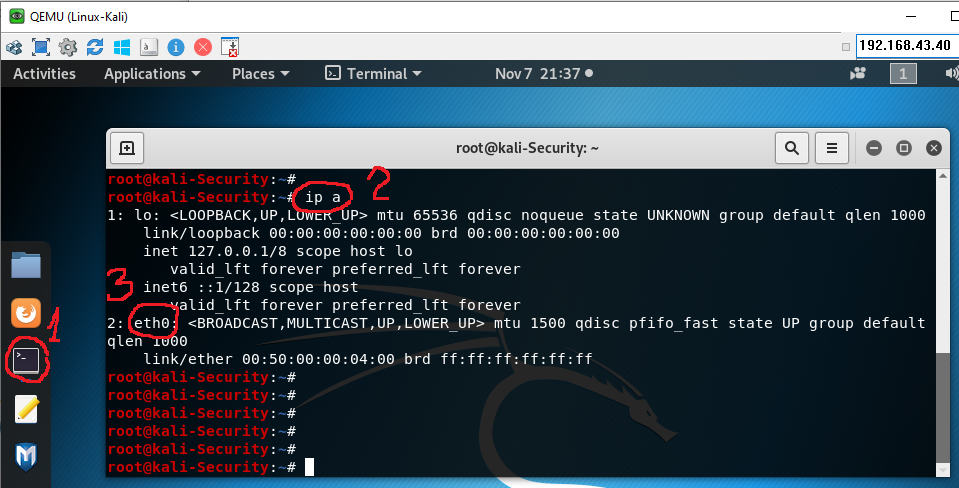


Рис. 21.

Чтобы настроить статический адрес воспользуемся графическим интерфейсом. Нажимаем кнопку (1) и в открывшемся окне выбираем (2).

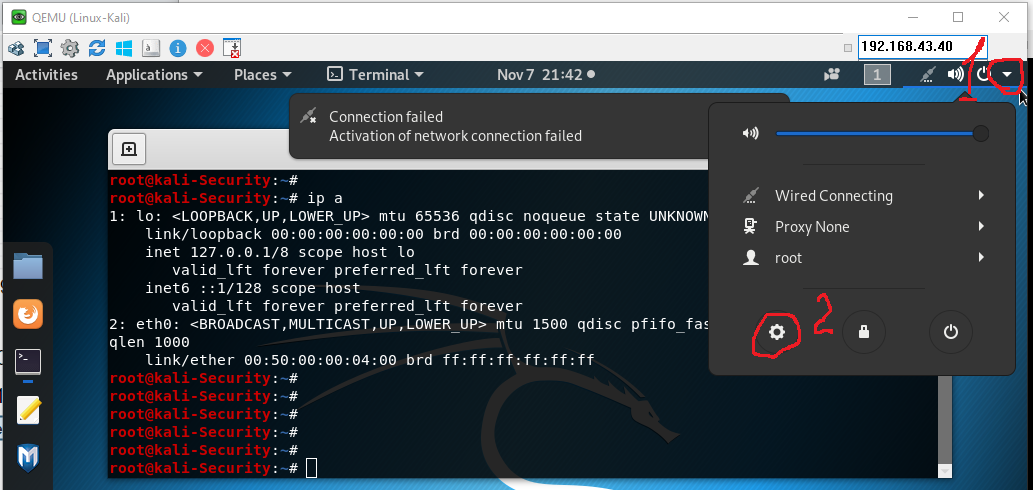


Рис. 22.

В открывшемся окне выбираем сеть (1) и настройки сети (2).

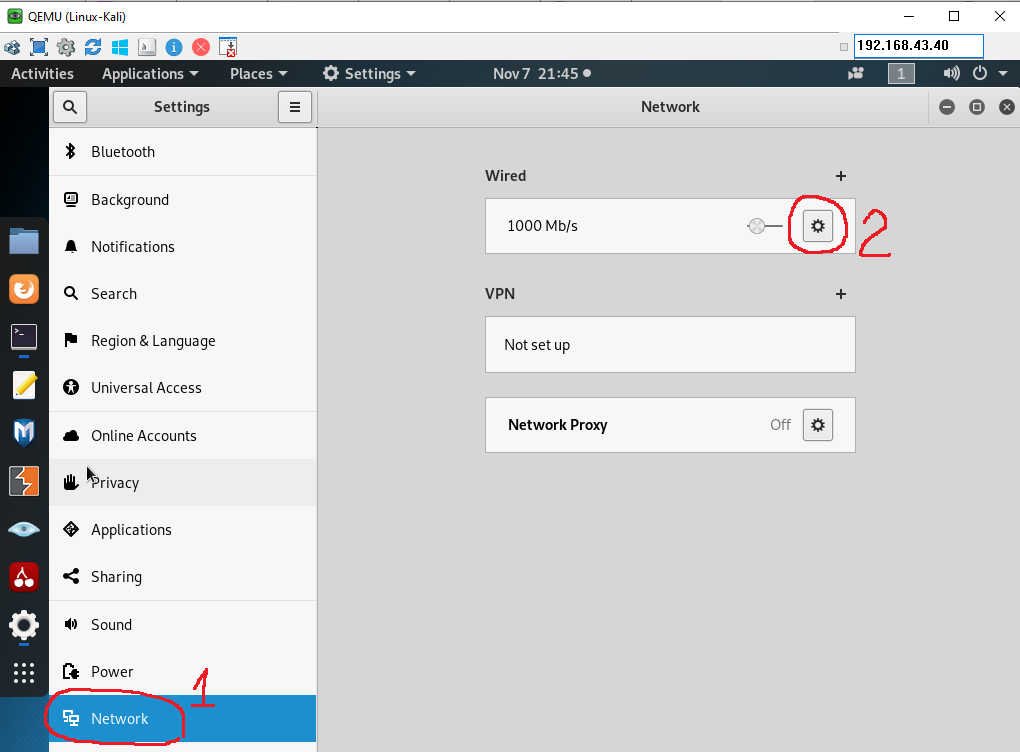


Рис. 23.

В открывшемся окне выбираем вкладку IPv4 (1), затем статическую настройку (2), адрес данного компьютера (3), его маску (4), шлюз по умолчанию (5) и DNS сервер (6).

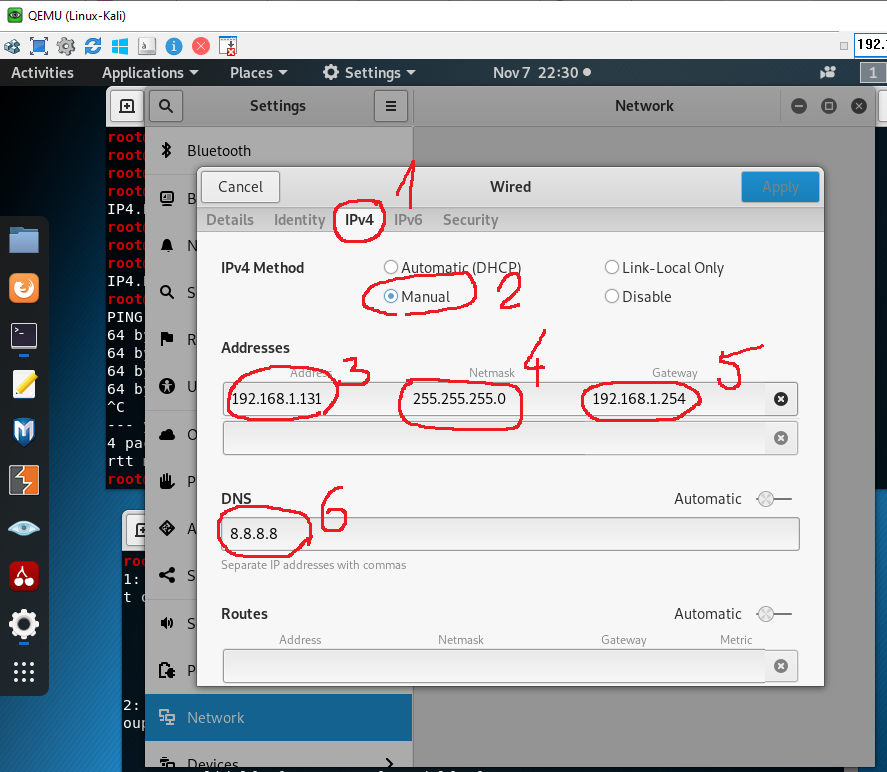


Рис. 24

Сохраняем изменения и проверяем.

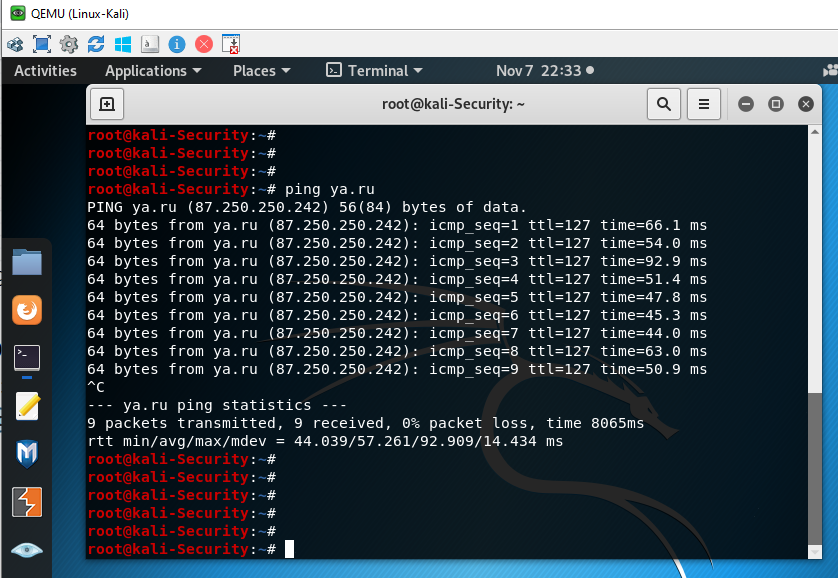


Рис. 25.

Теперь необходимо Kali превратить в роутер, чтобы можно было заниматься перехватом пакетов. Для этого заходим в системные настройки:



Рис. 26.

Необходимо снять комментарий со строки:

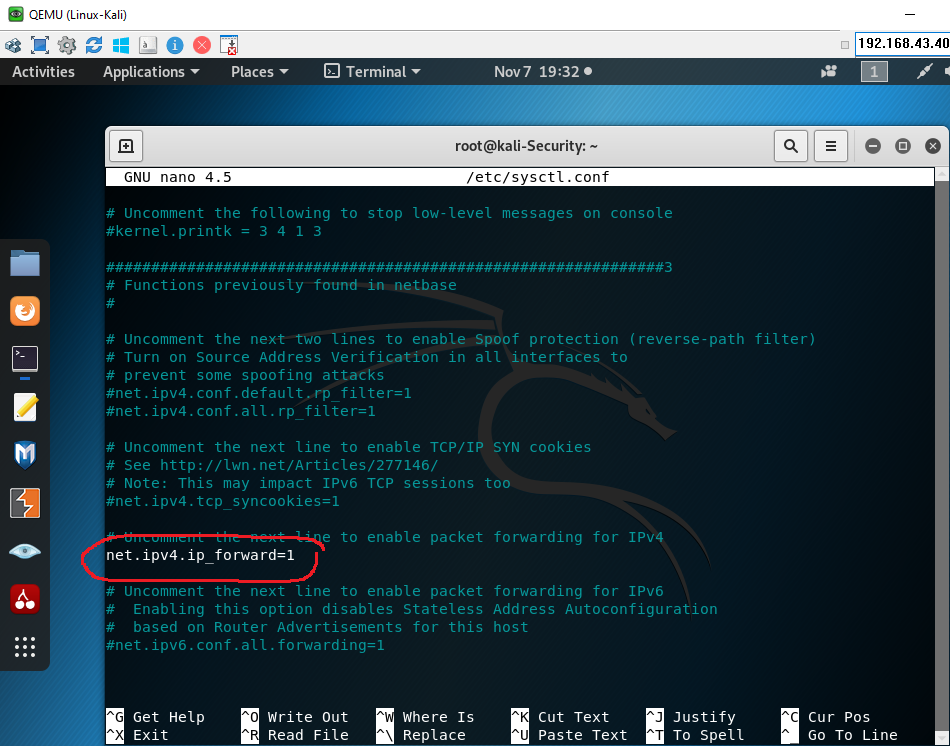


Рис. 27.

Необходимо сохранить этот файл и применить его командой sysctl –p



Рис. 28. 2:15:14

Таким образом мы включили возможность перенаправления трафика.

Теперь посмотрим arp-таблицу

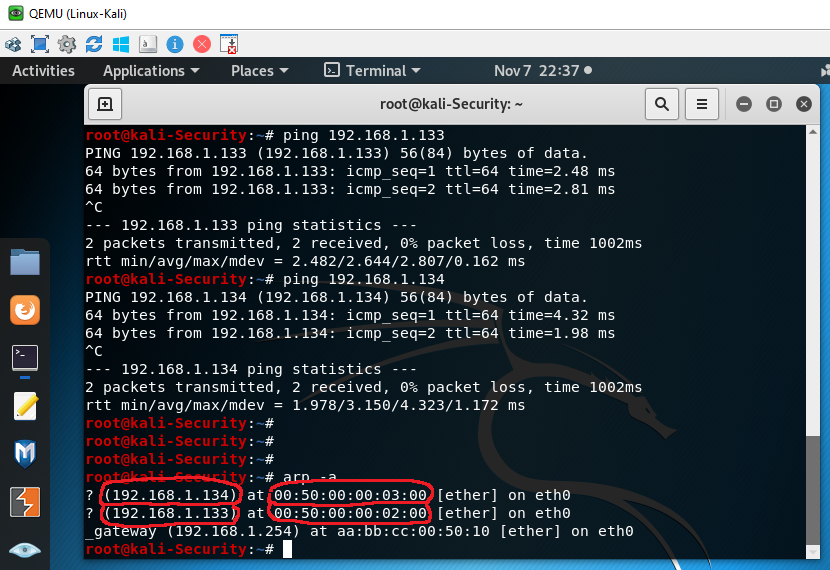


Рис. 29.

Мы видим ip-адреса и соответствующие им мас-адреса жертв. Теперь известно куда отправлять данные. Теперь запускаем атаку и будем смотреть какой трафик мы можем перехватить. Для этого используем утилиту arpspoof которая позволяет модифицировать arp-пакет.

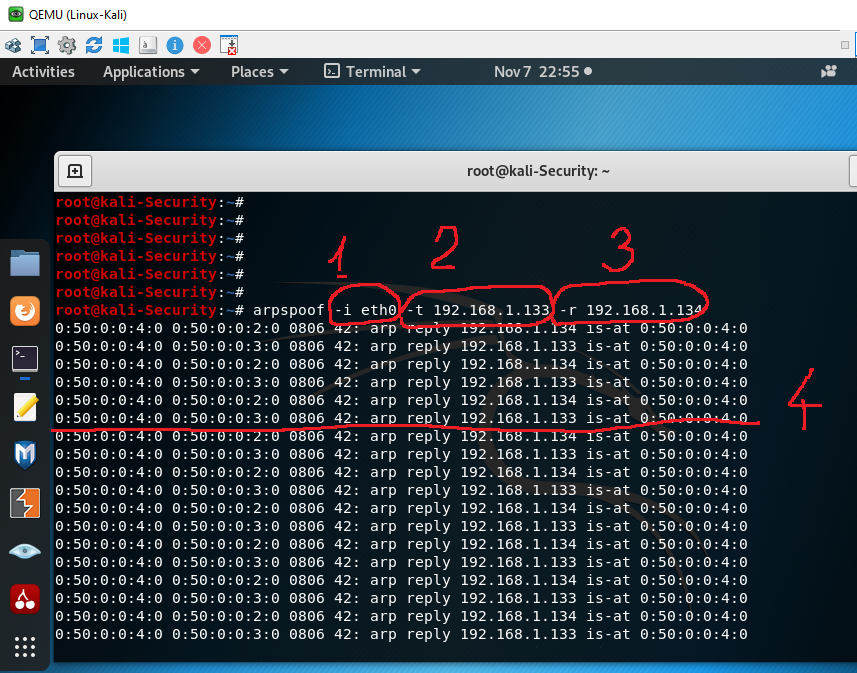


Рис. 30.

Первым параметром указывается интерфейс, с которого мы атакуем (1), соответственно (2 и 3) адреса атакуемых машин. При выполнении команды мы видим подмену адресов (4). Для анализа трафика используем программу wireshark

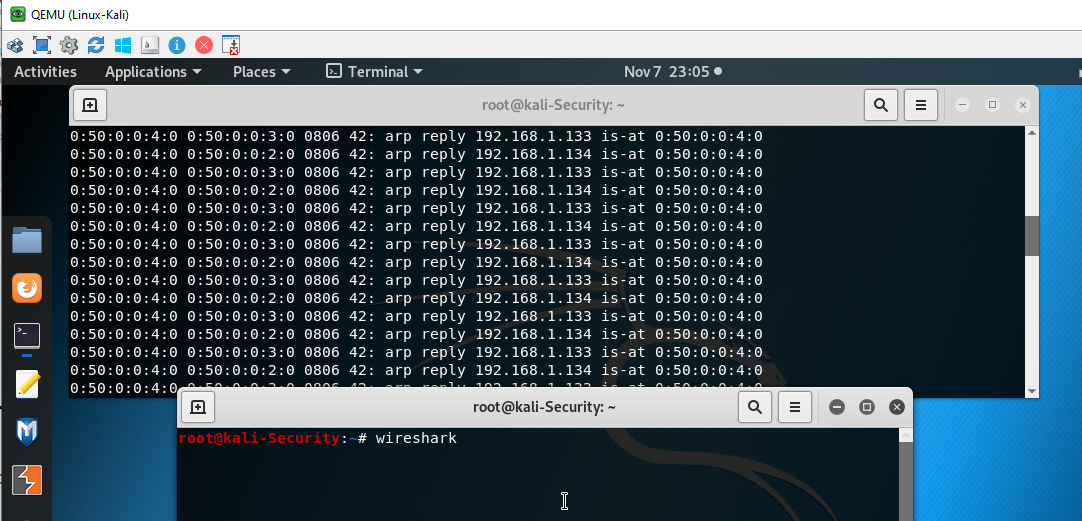


Рис. 31.

Вот что имеется на нулевом интерфейсе:

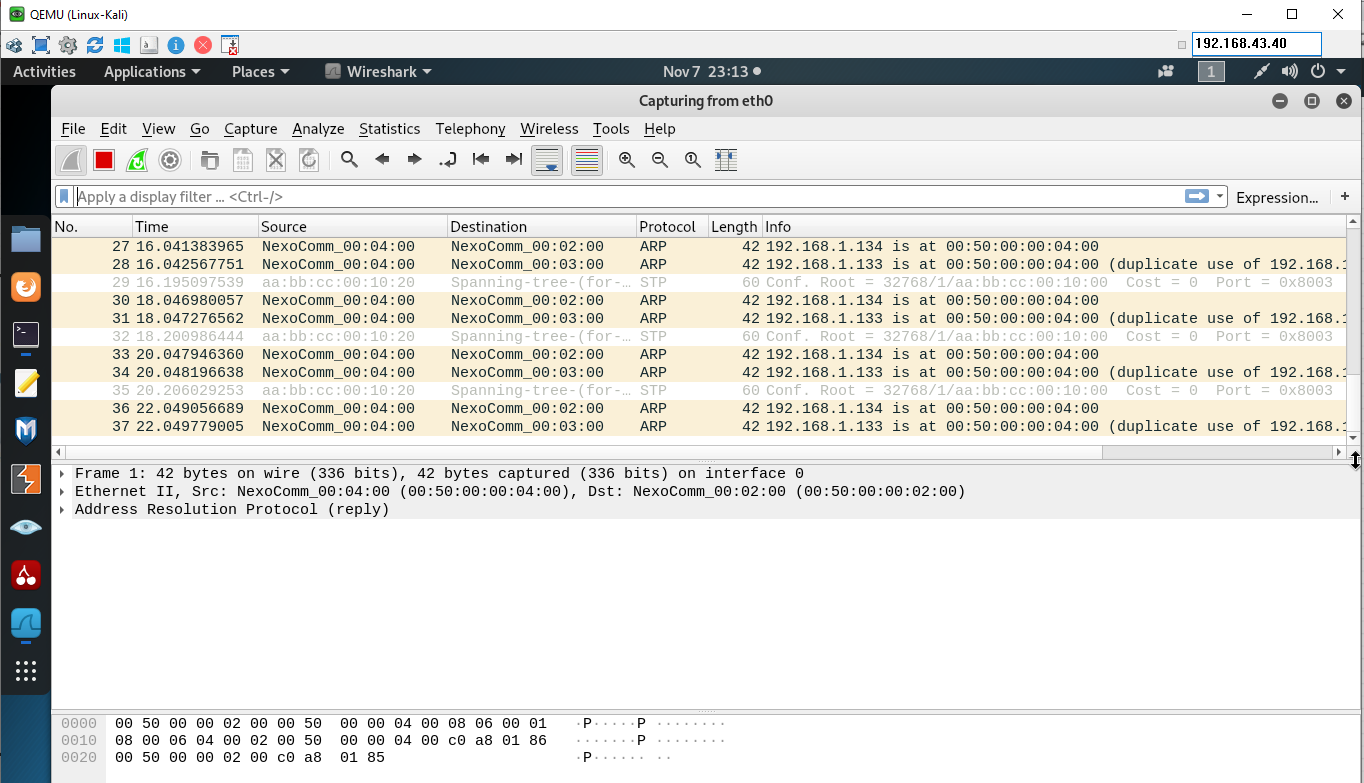


Рис. 32.

Включим фильтр по одному из атакуемых адресов и выполним пинг между атакуемыми машинами.

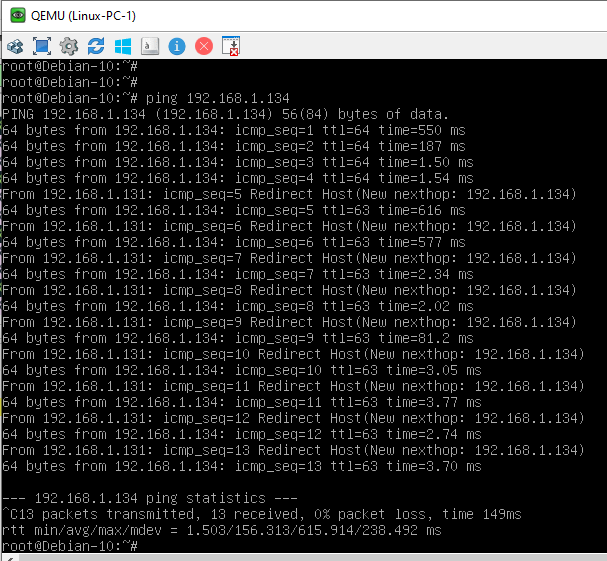


Рис. 33.

Wireshark также перехватывает пакеты

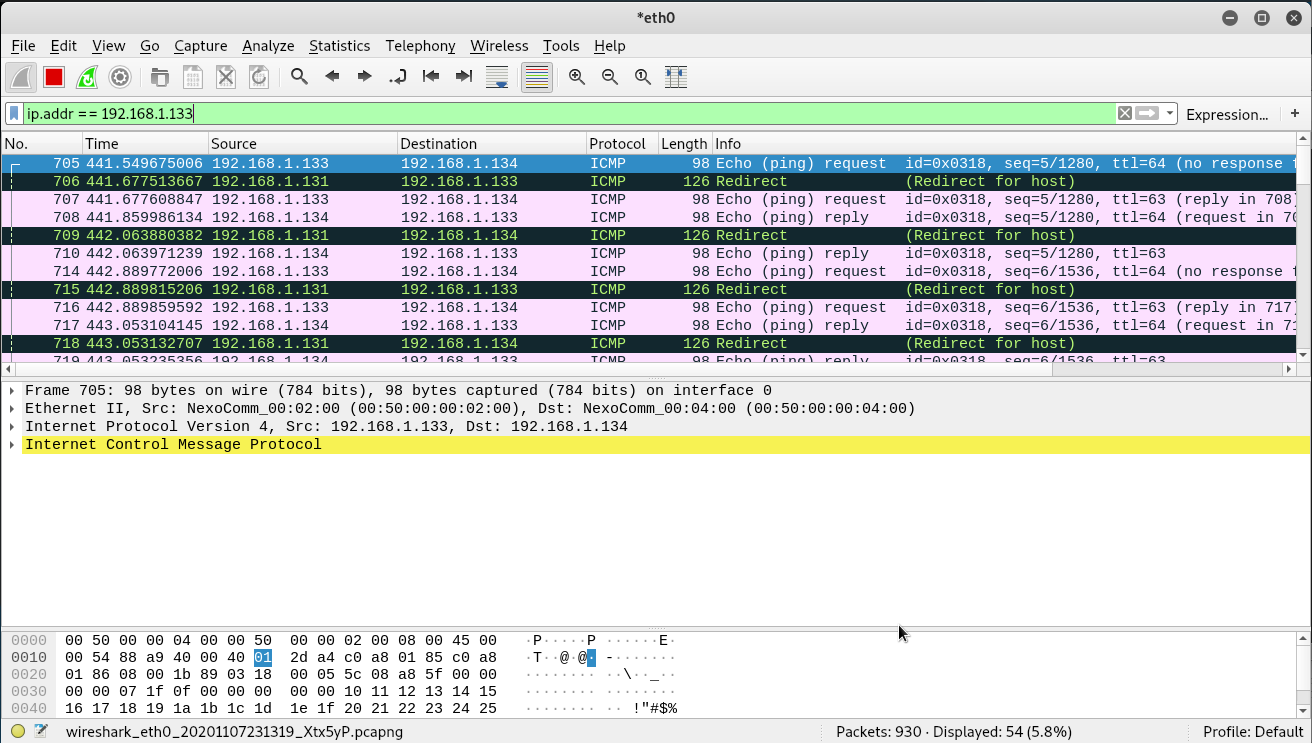


Рис. 34.

Если проанализировать пакеты, то все точно так, как описывалось в теории:

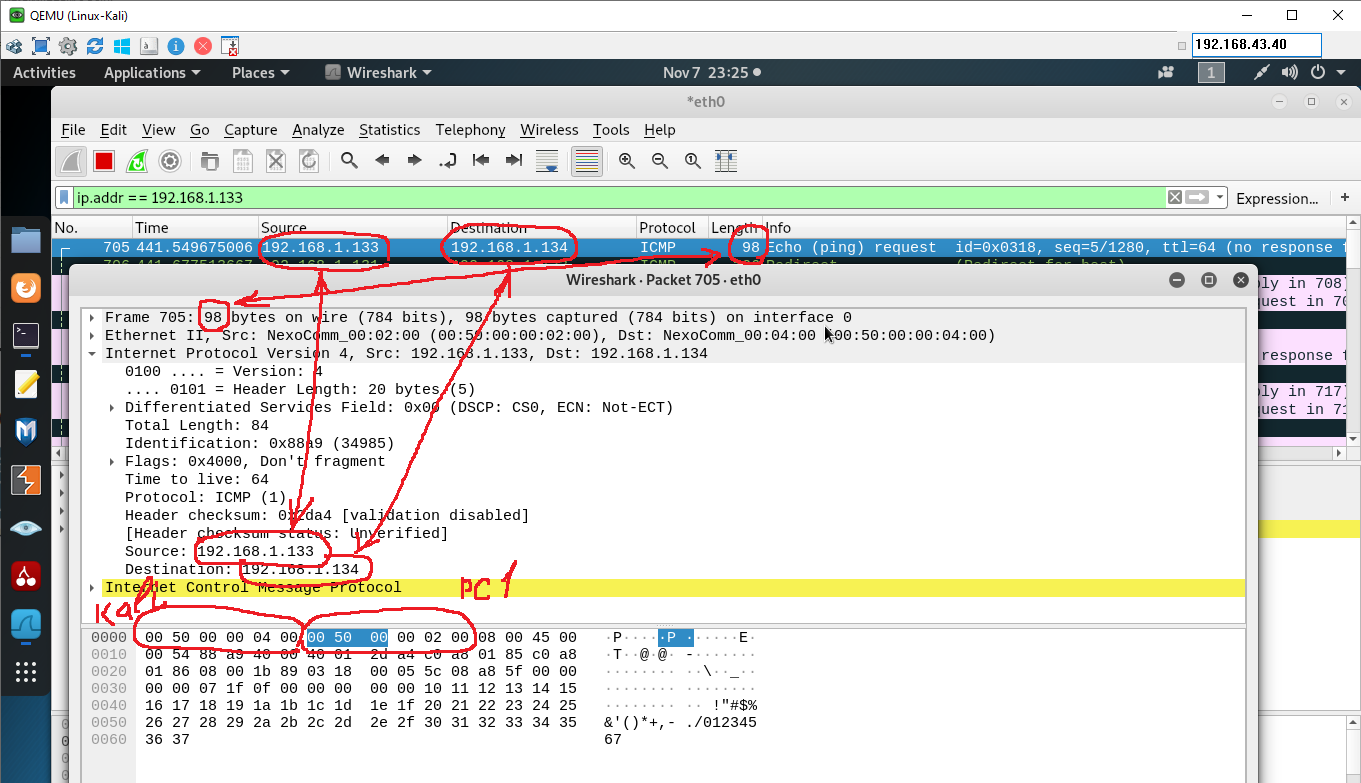


Рис. 35.

Если посмотреть таблицу arp на одной из машин, то мы увидим:

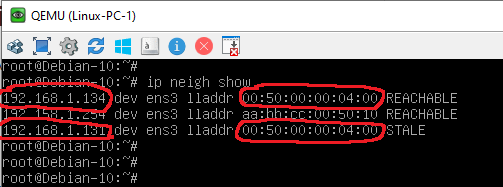


Рис. 36.

Пакеты с ip-адресами разных машин посылаются по одному и тому же мас-адресу.

Если посмотреть на кали, то видим что существует Redirect, который определяет перенаправление с кали на атакуемую машину.

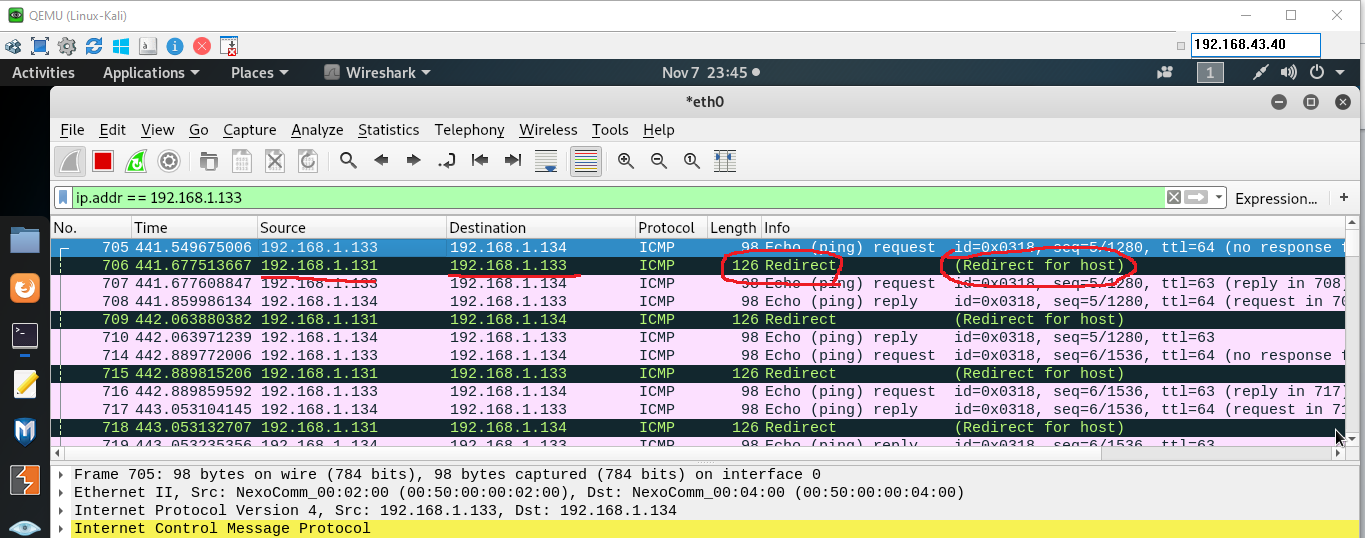


Рис. 37.

Таким образом мы перехватываем весь трафик между жертвами.