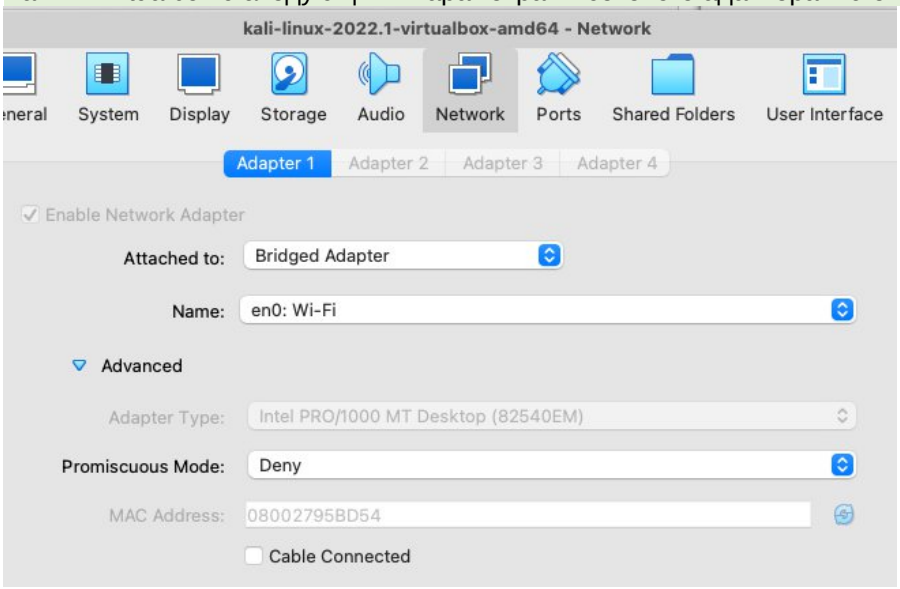
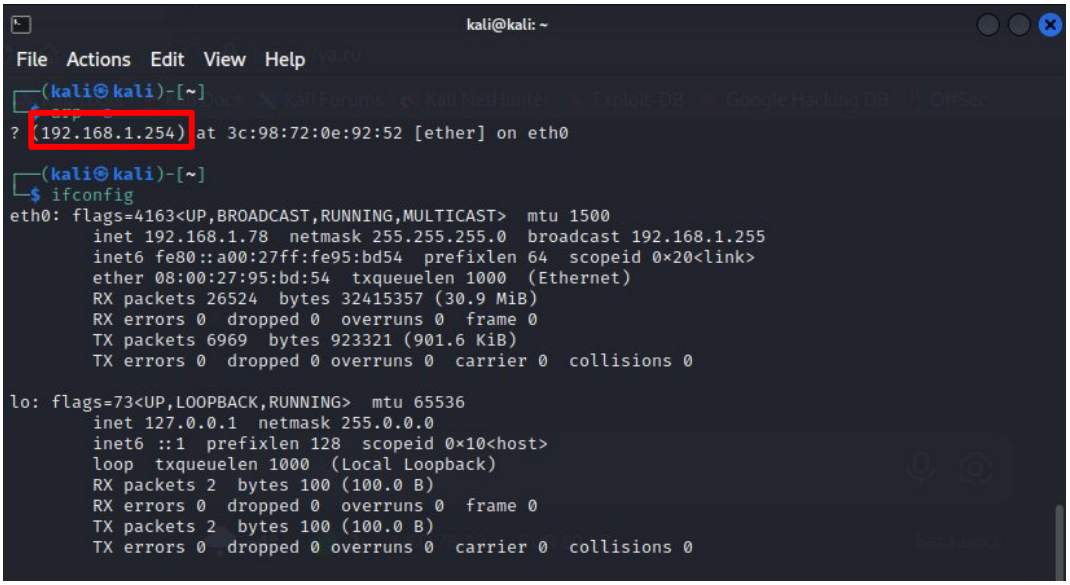
1. Поднять в одной сети две виртуальные машины: машину атакующего и машину жертвы. Требований по машинам, как рекомендация - сделать одну из машин (атакующего) kali.

Kali + Ubuntu

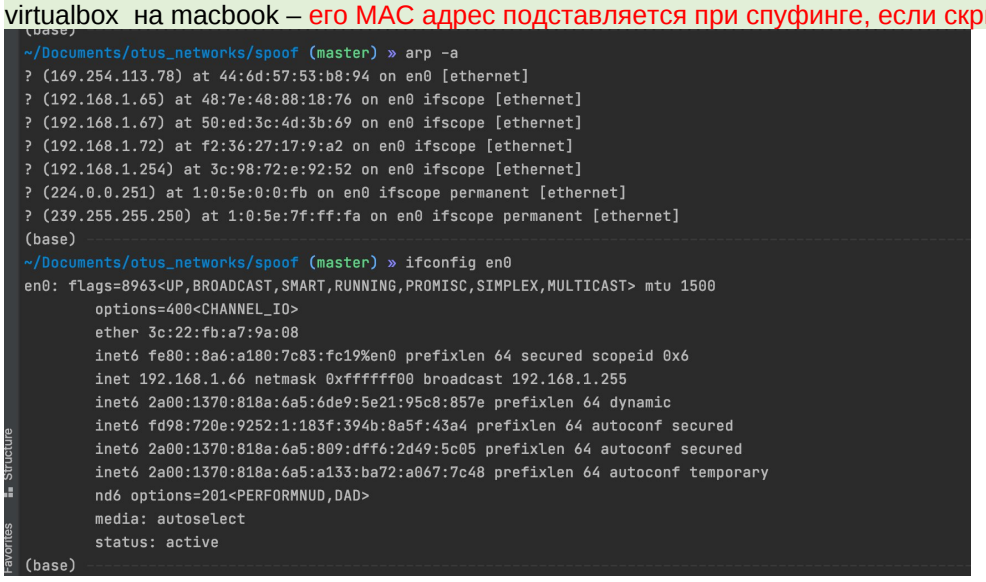
2. Исследовать ARP-таблицы и конфигурацию сети на обеих машинах, узнать адрес роутера.

Kali – в virtualbox с следующими параметрами сетевого адаптера и сгенерированным MAC

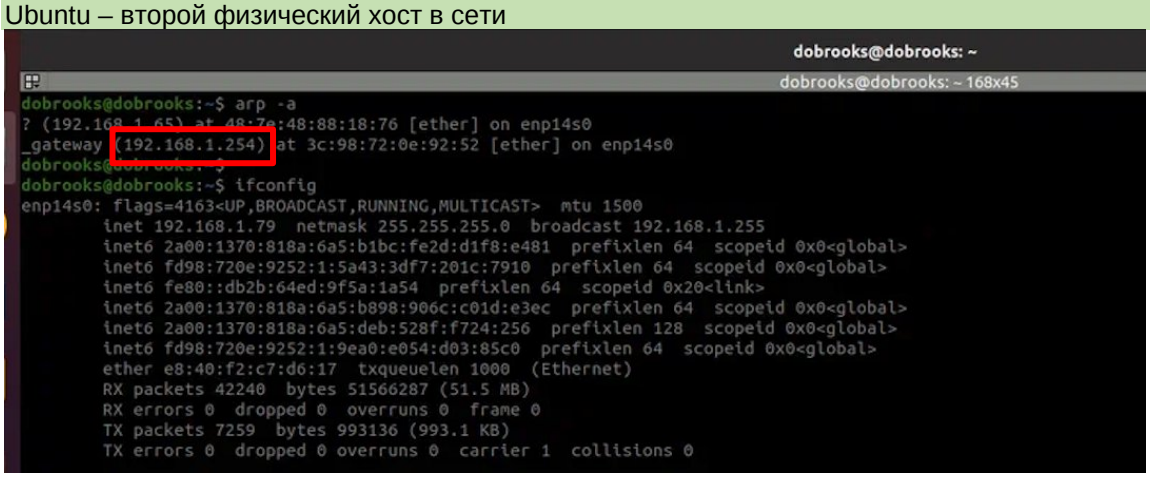




virtualbox на macbook – его MAC адрес подставляется при спуфинге, если скрипт запускать на kali

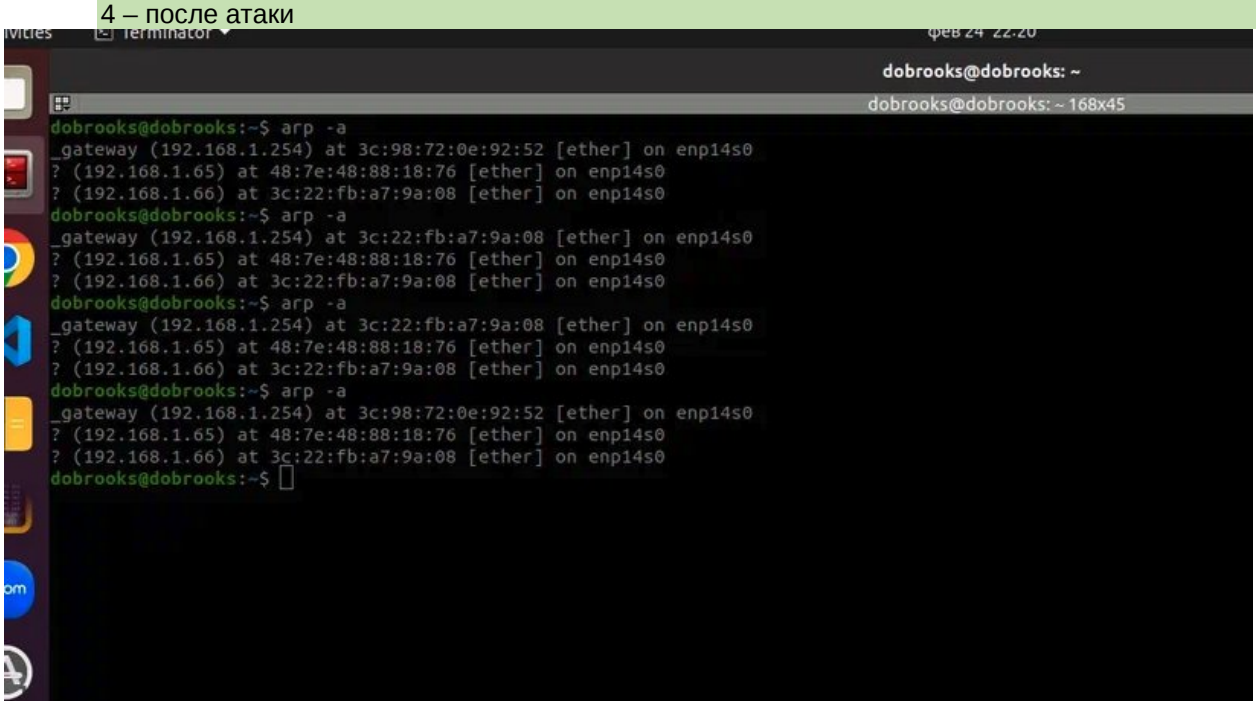


Ubuntu – второй физический хост в сети



Атакующий - 192.168.1.78
Атакуемый - 192.168.1.79
Роутер - 192.168.1.254

3. Необходимо подредактировать код arp_spoof.py (файл есть в материалах к занятию) таким образом, чтобы весь трафик машины-жертвы шел через машинку атакующего. На машине атакующего стоит проставить ip forwarding, чтобы на второй машине не пропало соединение с интернетом.
   +
4. Запустить написанный скрипт на машине жертвы и исследовать arp-таблицу на машине-жертве.
   + на машине жертвы? – запускал на атакующем хосте
5. Результатом выполнения домашнего задания должны стать три фала:
6. Доработанный файл с кодом arp_spoof.py.
   +
7. Скриншот arp-таблицы на машине-жертве во время работы скрипта.
   1- до атаки
   2 и 3 – во время атаки
   4 – после атаки



8. Advanced* (необязательное задание): написать функцию, восстанавливающую arp-таблицу на машине-жертвы после завершения атаки.

+
def change_table_back(target_ip, server_ip):