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
                                                  kali@kali: ~
 File Actions Edit View Help
  (192.168.1.254) at 3c:98:72:0e:92:52 [ether] on eth0
    -(kali⊕ kali)-[~]
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
         inet 192.168.1.78 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0×20link>
         ether 08:00:27:95:bd:54 txqueuelen 1000 (
RX packets 26524 bytes 32415357 (30.9 MiB)
                                                        (Ethernet)
         RX errors 0 dropped 0 overruns 0 frame 0
         TX packets 6969 bytes 923321 (901.6 KiB)
         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
         inet 127.0.0.1 netmask 255.0.0.0
         inet6 :: 1 prefixlen 128 scopeid 0×10<host>
         loop txqueuelen 1000 (Local Loopback)
         RX packets 2 bytes 100 (100.0 B)
         RX errors 0 dropped 0 overruns 0
         TX packets 2 bytes 100 (100.0 B)
         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ubuntu

```
| dobrooks@dobrooks:~
| dobrooks@dobrooks:~ | february | dobrooks@dobrooks:~ | dobrooks@dobrooks:~ | february | dobrooks@dobrooks:~ | february | full | february | febru
```

Атакующий - 192.168.1.78 Атакуемый - 192.168.1.79 Роутер - 192.168.1.254

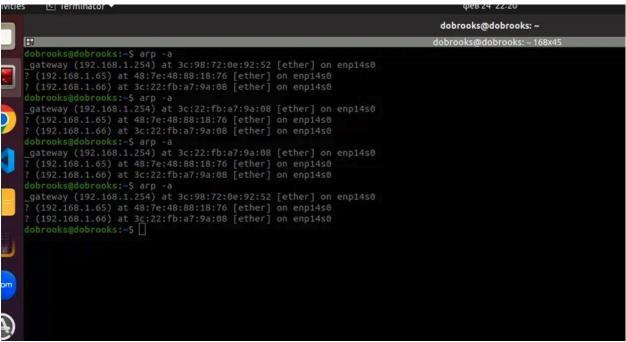
- 3. Необходимо подредактировать код arp_spoof.py (файл есть в материалах к занятию) таким образом, чтобы весь трафик машины-жертвы шел через машинку атакующего. На машине атакующего стоит проставить ip forwarding, чтобы на второй машине не пропало соединение с интернетом.
- 4. Запустить написанный скрипт на машине жертвы и исследовать агр-таблицу на машинежертве.

5. Результатом выполнения домашнего задания должны стать три фала:

6. Доработанный файл с кодом arp_spoof.py.

7. Скриншот агр-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 агр-таблицу на машине-жертвы после завершения атаки.

def change_table_back(target_ip, server_ip):