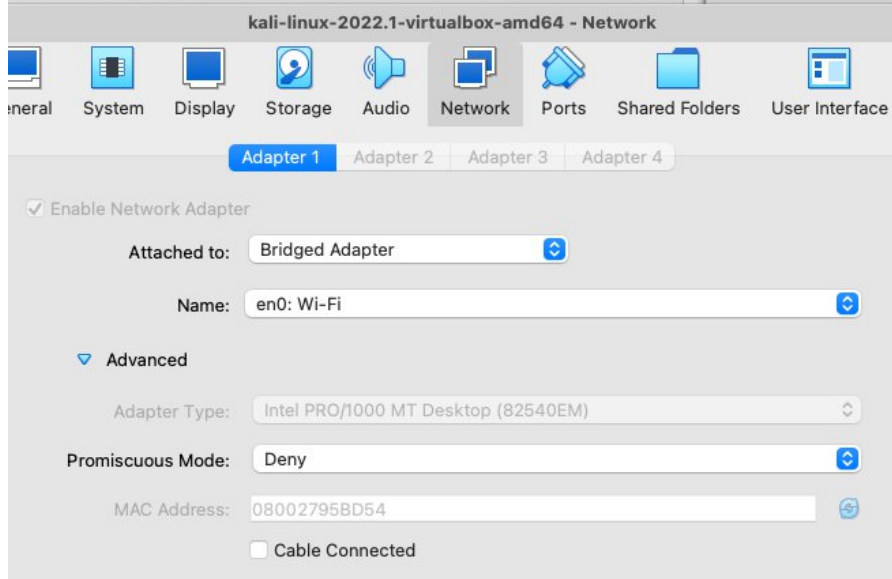


1. Поднять в одной сети две виртуальные машины: машину атакующего и машину жертвы. Требования по машинам, как рекомендация - сделать одну из машин (атакующего) kali.

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



```
kali@kali: ~  
File Actions Edit View Help  
~  
? (192.168.1.254) at 3c:98:72:0e:92:52 [ether] on eth0  
~  
$ ifconfig  
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 0x20<link>  
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)  
    RX packets 26524 bytes 32415357 (30.9 MiB)  
    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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2 bytes 100 (100.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2 bytes 100 (100.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
(base)  
~/Documents/otus_networks/spoof (master) » arp -a  
? (169.254.113.78) at 44:6d:57:53:b8:94 on en0 [ethernet]  
? (192.168.1.65) at 48:7e:48:88:18:76 on en0 ifscope [ethernet]  
? (192.168.1.67) at 50:ed:3c:4d:3b:69 on en0 ifscope [ethernet]  
? (192.168.1.72) at f2:36:27:17:9:a2 on en0 ifscope [ethernet]  
? (192.168.1.254) at 3c:98:72:e:92:52 on en0 ifscope [ethernet]  
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]  
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]  
(base)  
~/Documents/otus_networks/spoof (master) » ifconfig en0  
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500  
    options=400<CHANNEL_IO>  
    ether 3c:22:fb:a7:9a:08  
    inet6 fe80::8a6:a180:7c83:fc19%en0 prefixlen 64 secured scopeid 0x6  
    inet 192.168.1.66 netmask 0xfffff00 broadcast 192.168.1.255  
    inet6 2a00:1370:818a:6a5:6de9:5e21:95c8:857e prefixlen 64 dynamic  
    inet6 fd98:720e:9252:1:183f:394b:8a5f:43a4 prefixlen 64 autoconf secured  
    inet6 2a00:1370:818a:6a5:809:dff6:2d49:5c05 prefixlen 64 autoconf secured  
    inet6 2a00:1370:818a:6a5:a133:ba72:a067:7c48 prefixlen 64 autoconf temporary  
    nd6 options=201<PERFORMNUD,DAD>  
    media: autoselect  
    status: active  
(base)
```

```

dobrooks@dobrooks: ~
dobrooks@dobrooks: ~ 168x45
dobrooks@dobrooks:~$ arp -a
? (192.168.1.65) at 48:7e:48:88:18:76 [ether] on enp14s0
_gateway (192.168.1.254) at 3c:98:72:0e:92:52 [ether] on enp14s0
dobrooks@dobrooks:~$
dobrooks@dobrooks:~$ ifconfig
enp14s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.79 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2a00:1370:818a:6a5:b1bc:fe2d:d1f8:e481 prefixlen 64 scopeid 0x0<global>
    inet6 fd98:720e:9252:1:5a43:3df7:201c:7910 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::db2b:64ed:9f5a:1a54 prefixlen 64 scopeid 0x20<link>
    inet6 2a00:1370:818a:6a5:b898:906c:c01d:e3ec prefixlen 64 scopeid 0x0<global>
    inet6 2a00:1370:818a:6a5:deb:528f:f724:256 prefixlen 128 scopeid 0x0<global>
    inet6 fd98:720e:9252:1:9ea0:e054:d03:85c0 prefixlen 64 scopeid 0x0<global>
    ether e8:40:f2:c7:d6:17 txqueuelen 1000 (Ethernet)
    RX packets 42240 bytes 51566287 (51.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7259 bytes 993136 (993.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 1 collisions 0

```

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

```

dobrooks@dobrooks: ~
dobrooks@dobrooks: ~ 168x45
dobrooks@dobrooks:~$ arp -a
_gateway (192.168.1.254) at 3c:98:72:0e:92:52 [ether] on enp14s0
? (192.168.1.65) at 48:7e:48:88:18:76 [ether] on enp14s0
? (192.168.1.66) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
dobrooks@dobrooks:~$ arp -a
_gateway (192.168.1.254) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
? (192.168.1.65) at 48:7e:48:88:18:76 [ether] on enp14s0
? (192.168.1.66) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
dobrooks@dobrooks:~$ arp -a
_gateway (192.168.1.254) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
? (192.168.1.65) at 48:7e:48:88:18:76 [ether] on enp14s0
? (192.168.1.66) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
dobrooks@dobrooks:~$ arp -a
_gateway (192.168.1.254) at 3c:98:72:0e:92:52 [ether] on enp14s0
? (192.168.1.65) at 48:7e:48:88:18:76 [ether] on enp14s0
? (192.168.1.66) at 3c:22:fb:a7:9a:08 [ether] on enp14s0
dobrooks@dobrooks:~$

```

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

+
def change_table_back(target_ip, server_ip):