Switching and Person In The Middle attacks

Environment setup:

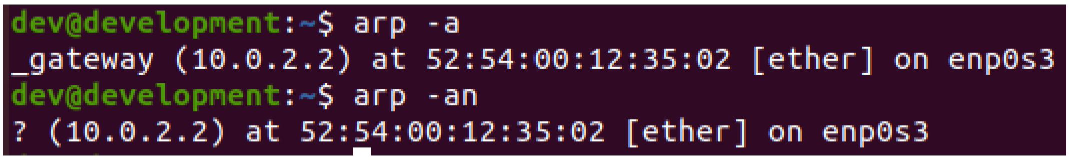
Download a Kali Linux OVA from here:
https://kali.download/virtual-images/kali-2021.3/kali-linux-2021.3-virtualbox-amd64.ova
Connect the machine’s NIC to Nat Network.
Check if the Kali machine can ping our “Webserver” and “Router” machines and debug the connection if needed.

ARP, Switching table, and ARP Table

As we learned on our 2nd layer lectures, the switch is memorizing MAC addresses in his LAN by **reading the source mac of every 2nd layer frame that arrives at his physical port**. The switch adds every newly learned MAC address to a table called Switching table, and matches the arriving MAC address to it’s correlative port. The switch “remembers” every MAC address for a preconfigured amount of time, and after the time is expired the table “forgets” the address.

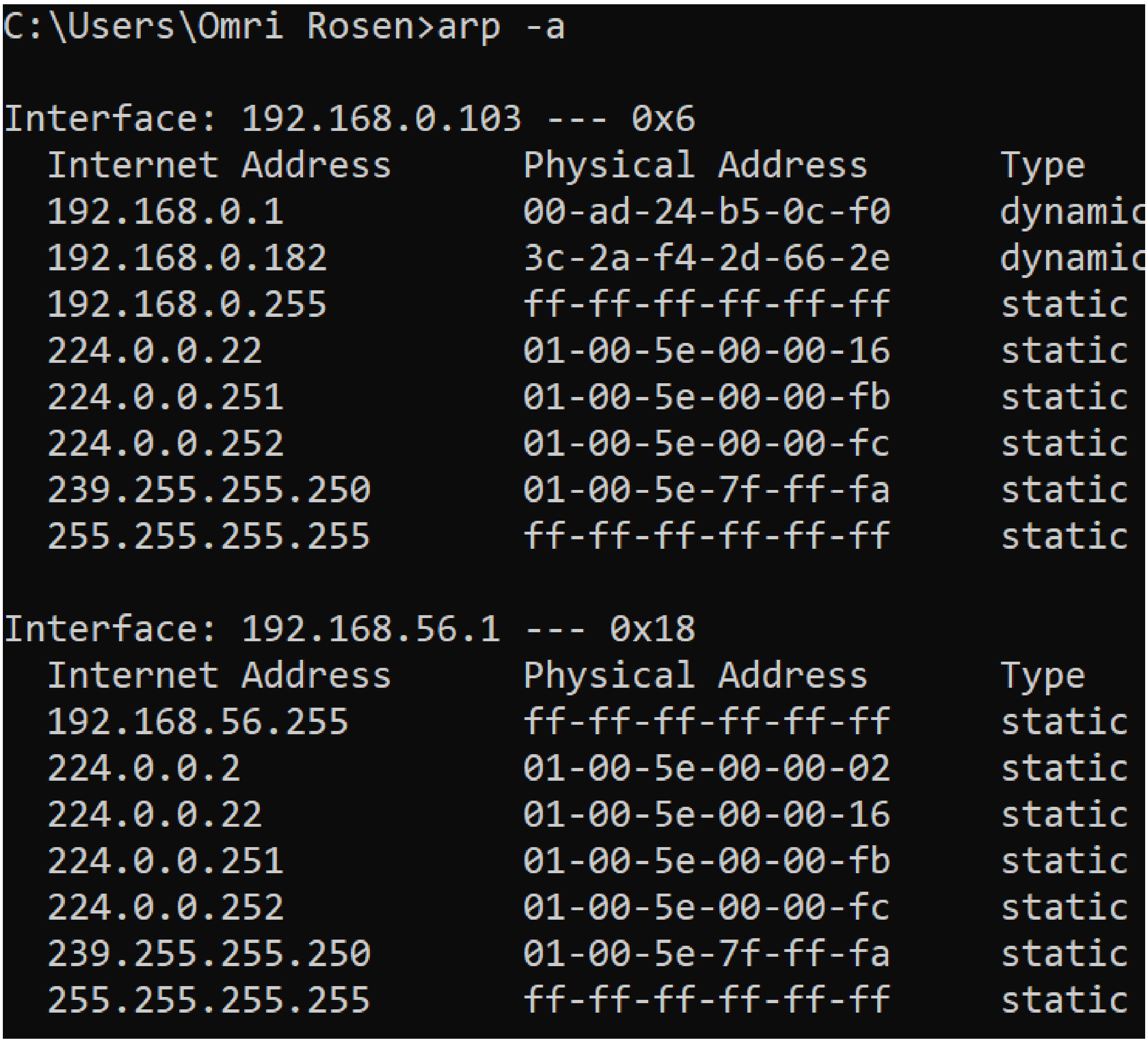
Every machine on the network needs to know it’s neighbour's MAC address in order to communicate. Usually the communication is driven by IP addresses. In order to **resolve** the MAC address associated with a certain IP address, the machine sends an ARP request (broadcast) frame. The machine with the IP we queried answers with an ARP reply, declaring the match between the requested IP address and the corresponding MAC address. To show a machine ARP Table use the command “arp -a”:

Linux:



```
dev@development:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
dev@development:~$ arp -an
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```

Windows:



```
C:\Users\Omri Rosen>arp -a

Interface: 192.168.0.103 --- 0x6
  Internet Address      Physical Address      Type
  192.168.0.1           00-ad-24-b5-0c-f0     dynamic
  192.168.0.182         3c-2a-f4-2d-66-2e     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x18
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

For further information about ARP protocol read Cisco CCNA course guide: https://study-ccna.com/arp/

Tasks:

- Open Wireshark on Kali and sniff your enp0s3 interface.
- Perform a PITM attack using the Kali machine and the Ettercap application.
- After performing the attack, find a way to assure the attack worked. You may run every command you like on every machine you like in the Nat Network LAN.
- Explain how you check if the attack worked.
- Draw a network diagram with all the tables and different types of addresses in our network before and after the attack.
- Explain in your own words, step by step, how the attack works. You should use your wireshark sniff.

- Bonus - after analyzing the attack, create an ARP poison python script to perform the attack. Your scripts should be able to receive the needed arguments for the attack in the command line as an argv.