Start pfsense, Kali, and metasploitable

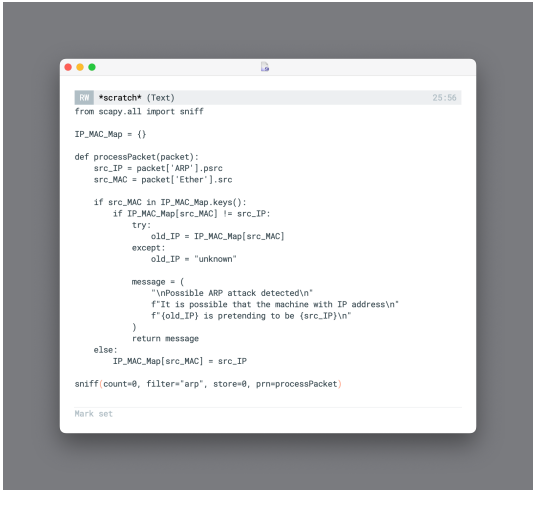
In Kali, install the `dsniff` tool [read the man page],
which includes `arpspoof` for intercepting network trafic.

Abstract steps you should take:

1. Find IP of the other machines on the network (hint: netdiscover)
2. Allow IP forwarding in Kali (hint: echo 1 > /proc/sys/net/ipv4/ip_forward)
3. Trick the victim: you're the router (hint: aspspoof -i eth0 -t <vict-ip> <router-ip>)
4. Examine the output of the command, which machine is each MAC
5. Trick the router: you're the victim
6. Generate some internet traffic in metasploitable (victim) (hint: wget)
7. Extract URLs from the victims computer (hint: urlsnarf)

Detect a spoofing attack

1. Install scapy[basic] in Kali
2. Write a python script using the sniff library from scapy



Exercises:

1. Inspect ARP tables in the metasploitable vm: sudo arp -a. Compare ART before and after attack.
2. Implement an ARP spoofer in python by consolidating all the individual steps you did in one command; i.e., you should be able to run python3 spoof.py <vict-ip> <router-ip> and it does everything.