Homework 3:

Firewall Exercise: Run the commands on Kali Linux VM. Do not forget to flush the rules after you have finished. Think and try traffic generation that can verify your rules. You may run the traffic from another VM (Metasploitable). For your report submit all the commands that you have run and include short description of your thought process and conclusions.

1. Assume you have two firewalls (FW1 and FW2), each with two Ethernet interfaces (eth0 and eth1).
   - FW1 protects the DMZ, and FW2 protects the LAN
   - Define an iptables policy for FW1 that：
     - Allows new Internet traffic to reach port 80 on 10.0.1.13
     - Does not allow traffic to reach the LAN (10.0.2.0/24)
   - Define an iptables policy for FW2 that:
     - Allows internal hosts to reach the webserver, but nothing else in the DMZ (10.0.1.0/24)
     - Prevents DMZ hosts from initiating connections to LAN

2. Assume you have a host with one network interface (eth0). You are running SSH (port 22) and want to allow access by external hosts. You are also running Apache for Web development, and only want it to be accessed by other hosts on the LAN (10.0.2.0/24)