IPTables

Description

In this project you will write various IP table rules to achieve the desired results. The following should be done on your suricata machine unless otherwise indicated.

1. Only allow 144.38.197.10 to access port 80 on that machine. (You should be able to login and verify via a wget)
2. Allow all hosts to ssh to that machine except for 144.38.197.10.
3. When a request is made to port 8080 on that machine, it should be answered by your client machine on that network (remember that your suricata assignment had the suricata machine and a client).
4. When a user tries to ssh to the suricata port 2222, redirect it to your client machine port 22.
5. When a user tries to ssh to the suricata port 2223, redirect it to 144.38.192.40 port 22.
6. Block outbound pings from your client (Hint: Use the `forward` chain)

TO pass off

Copy the output of the following commands to a file:

```
    iptables -vL -t filter
    iptables -vL -t nat
```