## Iptables

### Objective:

1. Learn how iptables work. In the process configure a firewall see how it works in practice.

### General instructions:

1. This lab can be done in any group size and can be discussed with any one ad nauseam
2. This lab is for learning purposes and there is nothing you need to submit.
3. Your learning will be tested via a written viva

### Reference:

1. Iptables notes and references as provided on bodhitree2.cse.iitb.ac.in

### Lab Instructions:

The below sections provide guidelines on what you need to implement and test. Designing the correct test and checking your implementation for all corner cases is your job. Attention to detail and thinking of corner cases is important here.

You will need atleast two machines with root access. More may help ease the process.

### Lab: Firewall

Your job is to use iptables and configure a firewall on a machine such that it can drop specific type of traffic. The different types of traffic to drop is listed below.

1. Drop all ping packets
2. Drop all TCP packets
3. Ensure no one can traceroute to the machine running the firewall.
4. Permit ssh from a designated IP address but from no other IP.
5. Permit traffic from a designated subnet but from no other subnet.

### Guidance:

1. Note each of the above bullet (type of traffic) is an independent experiment. Be sure to flush the iptables before you handle the next experiment.
2. Be sure to test each case by a) checking that before firewall everything is normal and b) after firewall the intended behaviour is observed.
3. Try to test with a variety of cases: contacting the firewall from different IP addresses, different subnets, use different protocols.