In-Class Exercise: Filter ICMP Packets

Week 6

In this exercise we will demonstrate how to use IPTables/NetFilter to filter out ICMP packets

1. Boot your VM system
2. Use either the terminal or make an SSH connection to your VM log into the VM system
3. Flush all existing rules in the VM

   sudo iptables –t filter –F

   sudo iptables –t nat –F

   sudo iptables –t mangle –F

4. Ping the VM either from the VM host or from a second VM (if you have one)

   ping -c 3 <vm_ip_address>

5. Check /proc/sys/net/ipv4/ip_forward in the VM

   cat /proc/sys/net/ipv4/ip_forward

6. If the value is not '1', sudo nano /proc/sys/net/ipv4/ip_forward
7. Filter ICMP packet being sent to the VM

   sudo iptables –A INPUT –p icmp –s <VM_host_ip_address> –d <vm_ip_address> –j DROP

8. Try to ping the VM

   ping -c 3 <vm_ip_address>