Requirements:

1.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1.View Default Chains | sudo iptables -L -t filter  sudo iptables -L -t nat  sudo iptables -L -t mangle |  |
| 2. See the Table and Chain Order | sudo iptables -t filter -A INPUT -j LOG --log-prefix filter-input  sudo iptables -t filter -A FORWARD -j LOG --log-prefix filter-forward  sudo iptables -t filter -A OUTPUT -j LOG --log-prefix filter-output  sudo iptables -t nat -A PREROUTING -j LOG --log-prefix nat-prerouting  sudo iptables -t nat -A INPUT -j LOG --log-prefix nat-input  sudo iptables -t nat -A OUTPUT -j LOG --log-prefix nat-output  sudo iptables -t nat -A POSTROUTING -j LOG --log-prefix nat-postrouting  sudo iptables -t mangle -A PREROUTING -j LOG --log-prefix mangle-prerouting  sudo iptables -t mangle -A INPUT -j LOG --log-prefix mangle-input  sudo iptables -t mangle -A FORWARD -j LOG --log-prefix mangle-forward  sudo iptables -t mangle -A OUTPUT -j LOG --log-prefix mangle-output  sudo iptables -t mangle -A POSTROUTING -j LOG --log-prefix mangle-postrouting |  |
| 3. Now, let's inspect the rules. | sudo iptables -L -t filter  sudo iptables -L -t nat  sudo iptables -L -t mangle |  |
| 4. Now let's test it out. Switch to the Fedora machine. | ping -c2 10.10.0.10  ping -c2 192.168.1.30 |  |
| 5. Now, switch back to the Debian machine. | sudo dmesg | grep 10.10.0.10 | grep 10.10.0.20 | grep TYPE=8 |  |
| 6. | sudo dmesg | grep 10.10.0.10 | grep 10.10.0.20 | grep TYPE=0 |  |
|  | sudo dmesg | grep 192.168.1.30 | grep TYPE=8 |  |
| Set Up NAT | Ubuntu machine ping -c2 8.8.8.8 |  |
| Switch back to Debian | sudo iptables -t nat -A POSTROUTING ! -d 10.10.0.0/24 -o eth0 -j SNAT --to-source 10.10.0.10  sudo iptables -t nat –L |  |
| Now let's test it. Switch to Ubuntu. | ping -c2 8.8.8.8 |  |
| Port Forwarding | sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT --to 192.168.1.30:22  sudo iptables -t nat –L |  |
| Connect via ssh to port 2222 on 10.10.0.10 | ssh -p 2222 10.10.0.10  ip a  exit |  |
| Basic Rate Limiting | nmap -p 1-100 10.10.0.10 |  |
|  | sudo iptables -N limit-port-scanning  sudo iptables -A limit-port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -m limit --limit 1/s --limit-burst 2 -j RETURN  sudo iptables -A limit-port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -j DROP  sudo iptables -I INPUT 1 -j limit-port-scanning  sudo iptables -L |  |
| Let's test the effect now. Switch back to Fedora. | nmap -p 1-100 10.10.0.10  sudo ping -f -c 100 10.10.0.10 |  |
| Hashlimit | sudo ping -f -c 100 10.10.0.10 |  |
| Switch back to Debian. | sudo iptables -A INPUT -p icmp -m hashlimit --hashlimit-name ICMPTEST --hashlimit-mode srcip --hashlimit-srcmask 32 --hashlimit-above 5/second --hashlimit-burst 2 --hashlimit-htable-expire 3000 -j DROP  sudo iptables –L |  |
| Switch back to Fedora | sudo ping -f -c 100 10.10.0.10 |  |
|  | sudo ping -A -c500 10.10.0.10 |  |
| Recent | sudo iptables -D INPUT 1  sudo iptables –L |  |
| Now switch to Fedora | ./test-ssh.sh |  |
| Now switch back to Debian | sudo iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set  sudo iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update --seconds 20 --hitcount 10 -j DROP  sudo iptables –L |  |
| Now switch to Fedora | ./test-ssh.sh |  |
| Connlimit - Add the following iptables rule. | sudo iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 2 -j REJECT  sudo iptables -L |  |