21. IPTABLES

Goal is to getting in touch with the basic functions of IPTABLES and to practice a few common firewall situations. You should figure out on your own how to set up firewall rules. Use the manpage of iptables for help and before you raise any questions.

For references please have a look at the web page put online at:
http://www.ks.uni-freiburg.de/download/inetworkSS05/practical/references/pra-ref06.html
Reminder: Please note that wireshark listens on the interface before the packets are filtered. Thus, incoming packets that get dropped are still shown in wireshark.

Question 1
First use command iptables -L, iptables -t nat -L, to look at the network traffic control rules in your host. Now block ping (ICMP) by using iptables. Try to ping anyone. Which additional consequences you or hosts connecting could suffer, if you block ICMP? Can you figure out how to configure iptables so that you are able to ping, but can't be pinged?

Question 2
Start a ssh server (/etc/init.d/ssh start). Try to block incoming connections to that server (port 22) using iptables! What is the difference between DROP and REJECT? Check it by connecting from another computer to the host that blocks the connections. Setup a firewall rule that just your partner(s) in the experiments session is able to connect to your machine but all the other "administrators" are blocked (this could be a trivial alternative to keep unwanted interference out instead of changing the password). Which alternatives you could think of to use instead of the source IP address?

Question 3
Now you should only allow one single ssh connection/host at the same time (the next session can connect from the moment on the first ended only).

Question 4
Now let's be evil ;) and fake our address when we ping. Remember IP Spoofing? For example, use iptables to modify your IP address to 10.230.4.x when sending out ICMP requests. Ping a friend and see what happens. (Your friend should take a look in wireshark, too). After that use as IP address 10.230.4.1 and analyse the generated traffic with wireshark. Are there any differences if you take an IP address which is in use elsewhere in the experiments subnet compared to an unclaimed address?

Question 5
Use nmap to scan for open ports on your neighbours machines. Which open ports do you observe? You should create a whitelist that blocks all incoming traffic except all allowed traffic.

1. Create an exception that allows only incoming traffic if there exists an outgoing connection.
2. Block all incoming traffic on any port and any protocol.

Question 6
Try to find out how many packets matched a certain rule of your firewall setup!

Solutions iptables:

1. Block ICMP: iptables -A INPUT -p icmp --icmp-type ping -j DROP
Unblock ICMP: iptables -D INPUT -p icmp --icmp-type ping -j DROP

2. SERVER-LAPTOP:
Install SSHd (openssh-server)
Run the SSH-server (/etc/init.d/ssh start)
sudo iptables -A INPUT -p tcp –dport 22 -s IP_Partner -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP

DROP: throws packet away, no notification
REJECT: rejects the paket, means the rejection will be announced: connection refused

3.
sudo iptables -A INPUT -p tcp --dport 22 -m connlimit --connlimit-above 1 -j REJECT

4.
(a) iptables -t nat -A POSTROUTING -o eth0.260 -p icmp -j SNAT --to <other ip>
(b) iptables -t nat -A POSTROUTING -o eth0.260 -p icmp -j SNAT --to <ip from the same group>

5.
zu 1.: iptables -A INPUT -p all -i eth0.260 -m state --state RELATED,ESTABLISHED -j ACCEPT
zu 2.: iptables -A INPUT -p all -i eth0.260 -j DROP

6.

sudo iptables -nvL

if you want you can use the -x flag, too.