1 Firewall policies for a honeynet (lab task)

Discuss your proposal with the group.

2 iptables exercises (homework)

For each of the following scenarios write a policy statement and the appropriate iptables rules to enforce the policy statement. Test your rules if possible. Submit your rules in a written form by the next session.

2.1 Scenario 1: Network management - 1 point

You are managing a network. You are supposed to block any traffic to the network except for ssh traffic.

2.2 Scenario 2: Remote server management - 1 point

You are managing a server on your network. This server is assigned IP address 192.168.0.15. It listens on ports 45679 and 56689. These ports must be reachable from the outside, while all other ports and hosts on the network must not be reachable.

2.3 Scenario 3: Internet Cafe - 1 point

You are running a small internet cafe. Therefore, you only want to allow pure HTTP and DNS (disregard HTTPS, ...). However, on Sundays all your PCs need to run a weekly update between 4:00 PM to 7:00 PM on port 24789. Make sure only connections that are initiated from inside your network are accepted.

2.4 Scenario 4: Honeynet firewall - 5 points

According to the policy discussed in class implement firewall rules to enforce this policy. Create an init script that will apply these rules on system start.