1 Firewall policies for a honeynet (lab task)

Discuss possible policies for a firewall used in a honeynet. Especially consider legal liabilities for damage done to systems outside the honeynet.

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 on the 17.11.2009.

2.1 Scenario 1: Network management

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

You are managing a server on your network. This server is assigned IP address 192.168.0.15. It listens on ports 45678 and 56789. 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

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 5:00 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

You are trying to protect the outside world from your honeynet. However, you also want to allow an attacker to download tools etc. to a compromised machine. Therefore, you need to allow a certain amount of TCP and UDP packets in the outgoing direction, while all incoming packets are allowed anyway.