Worksheet 3: Honeynet configuration & Sebek

04.05.2010, Garching

Due 11.05.2010

1 Honeypot configuration (lab task)

Give the group a short overview of your planned OS and services along with a description of vulnerable parts in your setup.

2 OS installation (homework)

Install your chosen operating system on your honeypot. Also start installing and configuring your services.

3 Sebek installation (homework)

Install Sebek on your honeypot. Make sure the network is still running afterwards and confirm that Sebek can be launched. Use port 6969 in your Sebek configuration. You can use tcpdump on your honeypot machine to confirm that Sebek packets are being sent. For now, the destination MAC address should be set to 00:00:00:FF:FF:FF and the target IP to 10.0.0.1.

4 Firewall policies (homework - 3 points)

Write down a possible policy for a firewall used in a honeynet. Especially consider legal liabilities for damage done to systems outside the honeynet. Hand in your proposal by the next session.