Worksheet 10:
Malware session and “opening the floodgates”

29.06.2010, Garching

Due 06.07.2010

1 Malware testing (lab task)

Make sure everybody has a working snapshot of their virtual machine and is ready for the test. Start capturing all traffic to and from your honeypot. Let your malware sample run. Restore your “clean” version after the session.

2 Traffic analysis (homework)

Look at the traffic your honeypot generated and received during the lab session. Did your malware sample create any packets? If yes, what was the malware author’s intent? Did the malware other groups used try to infect your machine? Write down a roundup of your findings and hand it in next session.