Worksheet 5: Tools

17.11.2009, Garching

Due 24.11.2009

1 MySQL (homework)

Write SQL statements for each of the following tasks:

1.1 Database creation

Create a database named according to your group name and two tables. Table #1 should be called “student” and contain three columns containing first and last name and a unique student ID number. Table #2 should be called “Groups” and contain a unique student ID number and a group name. Pick appropriate data types and primary keys within each table.

1.2 Data insertion

Write SQL statements inserting John Smith, student ID number 1234567, group 5 into the according tables. Do the same for Jane Doe, student ID number 2345678, group 7.

1.3 Data selection

Write a select statement that prints out all information on the students in group 5.

2 tcpdump (lab task)

Start tcpdump in such a way that it captures on eth1, writing its output to a maximum of 10 files with a maximum size of approximately 10 million bytes. Make sure you are capturing full packets (which does not hold true for the default settings). Use the man pages for reference.

3 p0f (lab task)

Use p0f reading from one of the files you captured with tcpdump.

4 snort (homework)

Go through the following tutorial: http://www-scf.usc.edu/~csci530l/instructions/lab-ids-instructions.htm