Worksheet 6: Monitoring

24.11.2009, Garching

Due 01.12.2009

1 Snort recycled (lab task)

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

The virtual machine image can be found at praksrv:/home/honeynet/snort_exercise/
The login name for this machine is “root”, the password is “password” (don't do this at home!)

2 Presentation (homework)

Prepare a 20 minute presentation for our next meeting. This presentation should answer the following questions:

a) Which operating system (version) and services did you choose?
b) What vulnerabilities exist in your chosen setup?
c) Are these vulnerabilities exploitable? If so, to what end? (E.g. remote execution, denial of service, ...)
d) Choose a vulnerability and a single exploit for it. How does the chosen exploit work in detail?
e) Is there malware “in the wild” which makes use of these exploits? If so, give examples!

Your presentation should include slides and you should be ready to answer questions afterwards. Any groups needing to borrow a laptop, coordinate with us before next Tuesday! Submit your slides until 01.12.2009, regardless of which slot you are going to give your presentation in.