1 Setup

You have been given credentials for the workstations as well as your honeypot. Make sure you can log in to both and change the passwords (command: `passwd`).

2 KVM

Familiarize yourself with the virtualization environment. Due to the way the networking is setup you will have to run KVM as root (`sudo`). Be sure you are able to:

- use VNC to access your VM’s display. (Hint: This will require you create a ssh tunnel as VNC does not natively support any sort of access control.)
- drop privileges to run as ‘student’.
- run KVM in the background without being killed when you log out.
- use a bridged network. (Hint: Use `-net nic` `-net tap` as options.)

Check the man pages and/or use the `-h` flag.

3 Create a Virtual Machine

Think about which operating system and services you want to offer on your honeypot. Create a virtual machine using KVM and begin installing these. You are responsible for getting the medium for the OS and services you want to install. For Microsoft products, we recommend MANIAC. The network will have to be statically setup (unless one of you decides to offer a DHCP server *cough* *cough*). The information for the network setup will be provided in class.

4 Subscribe to the Mailing List

Subscribe to the mailing list (each of you). You can do so by sending an email to `honeynet-praktikum-subscribe@sec.in.tum.de`. Once you are subscribed, share with us the ip address of your honeypot, the OS you will setup, and the services that you will make available.
5 Architecture (graded)

Think of an architecture for the honeynet and describe it. Give reasons for your design decisions. Also address any security concerns within your architecture and offer solutions to these concerns. Hand in your suggestion in a written form by the beginning of our next session. Be ready to discuss your reasoning.

6 Setup presentation (graded) [Due: 28.05.2013]

Prepare a 15 minute presentation. 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!
   If not, why is this vulnerability not being used by attackers?

Your presentation should include slides and you should be ready to answer questions afterwards.
Submit your slides by the beginning of the session on 28.05.2013.