Homework 4

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only one homework per email. Work in pairs and submit a single solution! CC the email to your partner. Please also submit only ASCII text or PDFs (no .docs etc). Every solution should be preceded by the corresponding question, like:

Qn:	**…a difficult question from me…**
A:	**…an answer from you …**
Q$n+1$	**…another difficult question…**
A:	**…another brilliant answer from you…**

Solutions will only be accepted until 20th December!

1. What should the architecture of a network application under Unix be that processes potentially hostile data?
2. What is a unikernel system and why is a unikernel preferable on a web server system (in contrast to a traditional general purpose operating system like Linux). Hint: What is the idea of a unikernel?
3. What does the principle of least privilege say?
4. How can you exploit the fact that every night root has a cron job that deletes the files in `/tmp`? (Hint: cron-attack)
5. In which of the following situations can the access control mechanism of Unix file permissions be used?
   (a) Alice wants to have her files readable, except for her office mates.
   (b) Bob and Sam want to share some secret files.
   (c) Root wants some of her files to be public.
6. Explain what is meant by *Kerckhoffs' principle*.
7. How can a system that separates between *users* and *root* be of any help with buffer overflow attacks?
8. What does it mean that the program `passwd` has the `setuid` bit set? Why is this necessary?
9. Under Unix (for example BSD Unix, MacOSX) the `login` programm has the setuid bit set. Why is this needed? In Linux `login` does *not* have the setuid bit set. What are the consequences of this choice?

10. The variable `PATH` is a shell variable in UNIX which lists all directories that should be automatically searched for a program. For example if `PATH` contains the directory `/usr/bin` and the program `ls` is stored there, then a user does not need to type `/usr/bin/ls` to run this file, but `ls` suffices. The question is why is it a bad idea in general, but in particular for root, to have `.` as the first entry in ones variable `PATH`?

11. In the context of which information flow should be protected, explain briefly the differences between the *read rule* of the Bell-LaPadula access policy and the Biba access policy. Do the same for the *write rule*.

12. **(Optional)** This question is for you to provide regular feedback to me, for example what were the most interesting, least interesting, or confusing parts in this lecture? Is there anything you like to have improved or explained in the handouts? Please feel free to share any other questions or concerns.