Homework 4

1. Explain what is meant by *Kerckhoffs' principle*.

2. How can a system that separates between *users* and *root* be of any help with buffer overflow attacks?

3. Consider the following simple mutual authentication protocol:

$$\begin{array}{ll} A \to B\colon & N_a \\ B \to A\colon & \{N_a, N_b\}_{K_{ab}} \\ A \to B\colon & N_b \end{array}$$

   Explain how an attacker B' can launch an impersonation attack by intercepting all messages for B and make A decrypt her own challenges.

4. Explain what are the differences between dictionary and brute forcing attacks against passwords.

5. 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*.

6. A Unix directory might look as follows:

```
$ ls -ld . * */*
drwxr-xr-x 1 ping staff  32768 Apr  2 2010 .
-rw----r-- 1 ping students  31359 Jul 24 2011 manual.txt
-r--rw--w- 1 bob students   4359 Jul 24 2011 report.txt
-rwsr--r-x 1 bob students 141359 Jun  1 2013 microedit
dr--r-xr-x 1 bob staff  32768 Jul 23 2011 src
-rw-r--r-- 1 bob staff  81359 Feb 28 2012 src/code.c
-r--rw---- 1 emma students    959 Jan 23 2012 src/code.h
```

   with group memberships assigned as follows:

Members of group staff:	ping, bob, emma
Members of group students:	emma

   The file microedit is a text editor, which allows its users to open, edit and save files. Note carefully that microedit has set its setuid flag. Fill in the access control matrix below that shows for each of the above five files, whether ping, bob, or emma are able to obtain the right to read (R) or replace (W) its contents using the editor microedit.

	manual.txt	report.txt	microedit	src/code.c	src/code.h
ping					
bob					
emma					