

# LULEÅ TEKNISKA UNIVERSITET

Tentamen i

**Computer System Security and Management**

Antal problem: 8

Lärare: Pawel Pietrzak, 076-1410834

Resultatet anslås senast 2010-11-23 i A-huset.

Kurskod	D0004E/SMD139/102
Datum	2010-10-30
Skrivtid	4 tim

Tillåtna hjälpmedel: None

---

The limit to pass the exam will be around half of the total points. The answers can be written either in English or in Swedish.

---

## 1. DNS

Explain what the following DNS records specify:

- a) SOA
- b) NS
- c) A
- d) PTR
- e) MX
- f) CNAME

(4p)

## 2. Storage

- a) Describe each of the following raid levels and their most important characteristics in terms of performance and redundancy (*feel free to draw pictures to illustrate*): Raid 0, Raid 1, Raid 5. (3p)
- b) Why is it important to keep backups, even if the disks are mirrored? (2p)

(5p)

## 3. Mail

Assume you want to send an email to user@foo.tld using SMTP and your mail client is setup to send outgoing messages to smtp.bar.com for further delivery.

- a) How do you find out which mail server that would receive the message on the recipient side?
- b) If that server is not responding, what will happen with the message?

(4p)

4. **UNIX Systems** Assume your primary group is “users”. You are also a member of the group “staff”. Your `umask` is set to 022. If you create an empty file in your home directory, `ls -l` will produce the following output:

```
-rw-r--r--    1  bear      users          0 Oct 30  09:00  empty_file
```

After creating a directory `data` the command `ls -l` will give:

```
-rw-r--r--    1  bear      users          0 Oct 30  09:00  empty_file
drwxr-xr-x    1  bear      users         68 Oct 30  09:01  data
```

- a) Which users can remove files from the directory `data` ?
- b) Which users can remove files from the directory `data` after executing  
`chmod 775 data`  
`chgrp staff data`  
?
- c) Which users can remove files from the directory `data` after executing  
`chmod 775 data`  
`chgrp staff data`  
`chmod +t data`  
?

(3p)

## 5. Security

- a) What is stack smashing attack?
- b) Describe at least one way to prevent injecting executable code into a stack area.

(5p)

## 6. Security II

What are the three main security goals that two parties want to establish when communicating with each other?

(2p)

## 7. Cryptography

Explain why it is not a good idea to use a one-time pad twice. Use  $\oplus$  (XOR) in your answer.

(3p)

## 8. Script - Foo daemon

Write a start script for `/usr/local/sbin/food`, the foo daemon. This daemon behaves well, and will always write its pid to `/var/run/food.pid`, as well as deleting the file upon exit. The script should start `/usr/local/sbin/food` if it is called with `start` as an argument, and kill it if it is called with a `stop` argument.

**NOTE:** *Extracts from the man pages to bash are appended.*

(4p)

GOOD LUCK!