

# LULEÅ TEKNISKA UNIVERSITET

Tentamen i

**Computer System Security and Management**

Antal problem: 7

Lärare: Simon Aittamaa, 070-3593922

Resultatet anslås senast 2009-11-15 i A-huset.

Kurskod	D0004E/SMD139/102
Datum	2009-10-27
Skrivtid	4 tim

Tillåtna hjälpmedel: Inga

---

The limit to pass the exam will be around half of the total points. An additional requirement is that you have a **minimum of three points from question one**, otherwise the remaining answers will not be graded.

---

## 1. Cryptography

Explain the important characteristics of:

- Symmetric encryption
- Asymmetric encryption
- Message Digest
- One time pad
- How is cryptography used in SSH?

(5p)

## 2. DNS

What type of DNS-records have the following functions?

- Name to address translation
- Identifies name servers
- Controls e-mail routing
- Address to name translation
- Aliases for a host

(5p)

## 3. Storage

Describe the different 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

(4p)

#### 4. Security

Consider a typical web application, somewhere containing the statement:

```
statement := "SELECT * FROM users WHERE name = '" + userName + "';"
```

Explain how this can be exploited if the contents of *userName* is not checked before executing this statement.

(3p)

#### 5. UNIX Systems

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
henrik:x:0:0:Henrik:/home/henrik:/bin/bash
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
sshd:x:100:65534:./var/run/sshd:/bin/false
bind:x:101:101:./var/cache/bind:/bin/false
martin:x:1000:1000:Martin,,,:/home/martin:/bin/bash
```

- What is the traditional Unix name of the file that holds the content that is showed above, and where can you usually find it?
- What is the traditional Unix name of the file that holds the content that is showed beneath, and where can you usually find it?
- In both files, one line holds a number of fields separated by a colon. Explain what each field represents (going left to right) in the two files.
- The file above is copied from a stationary desktop computer with one user. Based on this information, can you identify something that may be suspicious with this file?

```
wheel:*:0:root,rachel
uucp:*:10:uucp
users:*:100:
vision:*:101:keith,arlin,janice
startrek:*:102:janice,karen,arlin
```

(5p)

#### 6. 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.

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

(5p)

## 7. 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.*

(3p)

GOOD LUCK!