

LULEÅ TEKNISKA UNIVERSITET

Tentamen i

Computer System Security and Management

Antal problem: 7

Lärare: Peter A. Jonsson, 491638

Resultatet anslås senast 2008-11-05 i A-huset.

Tillåtna hjälpmedel: Inga

Kurskod	D0004E/SMD139/102
Datum	2008-10-23
Skrivtid	4 tim

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:

- a) Symmetric encryption
- b) Asymmetric encryption
- c) Message Digest
- d) One time pad
- e) How is cryptography used in SSH?

(5p)

2. DNS

Explain what the following DNS records specify:

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

(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*).

- a) Raid 0
- b) Raid 1
- c) 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. Hash Functions

a) Which of the following algorithms have known weaknesses (1p)

- MD5
- SHA-0
- SHA-1
- SHA-2

b) Is it wise to use an algorithm with a known weakness? Motivate! (2p)

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.

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?

(5p)

7. Script - Count Disabled Users

Write a shell-script that counts the number of users in /etc/passwd that are disabled in such a way that the string "***2007**" is the first part of the password field. An example of the format of passwd:

```
sven:p31TpxCa/.:9993:20:Sven Svensson:/home/sven:/usr/local/bin/tcsh
```

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

(5p)

GOOD LUCK!