

LULEÅ TEKNISKA UNIVERSITET

Tentamen i

Computer System Security and Management

Antal problem: 7

Lärare: Peter A. Jonsson, 491638

Resultatet anslås senast 2007-12-31 i A-huset.

Kurskod	D0004E/SMD139/102
Datum	2007-12-17
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 File permission

- a) What does it mean to run an application in a chrooted environment?
- b) What does it mean that a directory has the “sticky” bit set?
- c) What are the security implications of files that have the “setuid” bit set (2p)?
- d) Why is it good to check which user accounts that have userid 0 on a regular basis?

(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.

- 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 - 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!