

LULEÅ TEKNISKA UNIVERSITET

Tentamen i

Computer System Security and Management

Antal problem: 6

Lärare: Peter A. Jonsson, 491638

Resultatet anses senast 2007-11-15 i A-huset.

| | |
|----------|-------------------|
| Kurskod | D0004E/SMD139/102 |
| Datum | 2007-11-01 |
| 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:

- 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

(6p)

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.

(5p)

5. UNIX Systems

- a) When you log in to a machine your SSH client tells you:

```
The authenticity of host 'machine.sm.ltu.se (130.240.2.100)' can't be established.  
RSA key fingerprint is 1c:48:d3:43:d3:4d:6a:05:24:e8:84:95:77:30:f0:ba.  
Are you sure you want to continue connecting (yes/no)?
```

What does this message mean? How is it possible to establish the authenticity of host?

(2p)

- b) Assuming that you once have successfully established a connection to the machine, the next time you connect to the same machine you get the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that the RSA host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
2e:04:e6:06:c2:1a:ee:b1:71:c9:ec:b7:76:d7:21:46.  
Please contact your system administrator.  
Add correct host key in /home/user/.ssh/known_hosts to get rid of this message.  
Offending key in /home/user/.ssh/known_hosts:218  
RSA host key for erwin.dc has changed and you have requested strict checking.  
Host key verification failed.
```

Why does this occur? Give two scenarios when you can get this message.

(3p)

6. 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!