# Systems and Network Security Final Exam

| Date | : 24.07.2008 |
|---|---|
| Duration | : 120 Mins. |

| Q1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 10 | 10 | 5 | 10 | 5 | 10 | 10 | 10 | 10 | 5 | 5 | 10 | 5 | 5 | 5 | 120 Pts. |

## Questions

**1)** Explain the term “low hanging fruit”. **(5 Pts.)**

**2)** What is a path killer? Why is it important for risk management? **(10 Pts.)**

**3)** What is the security problem in using multiple SAP R/3 instances on one application server? How can this be remediated? **(10 Pts.)**

**4)** From: **kernel/exit.c**

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
                retval = -EINVAL;
```

The above code was found in Linux kernel before it went live. What is the security flaw? **(5 Pts.)**

**Note:** **__WCLONE** and **__WALL** are flags that can be passed by a user.

**5)** Explain the methods that can be used to execute OS commands using Oracle Databases. **(10 Pts.)**

**6)** How can an attacker use HSRP to execute a man in the middle attack? **(5 Pts.)**

**7)** Why are ssl certificate errors critical? What would you recommend to a company who gets these errors, even though no attack is taking place? **(10 Pts.)**

**8)** Thomas Ptacek | July 8th, 2008

**Java JSESSIONID**: BB16479A0338D3DCF26D11712F138BC1

**.NET ASPESSIONID**: HHODHGFDJOJAKDIPPJCKHGOE

**SiteMinder SMESSIONID**: su/hxP2nLeaZQpSCSxKYBLVTF[…]O93DX/I82bQ3mcCco

**DNS XID**: 04d8

**Getting To File This Week’s Front Page Security Story Before Changing Out Of Your Pajamas**: Priceless.

What is Thomas Ptacek referring to? What could be the security issue? Explain in details how you think this can be exploited and what can be achieved. **(10 Pts.)**

**9)** You are at location A with a box, a padlock with its key and a secret document. You have someone at location B, who also has a box of equal size, a padlock with its key and she needs to have the secret document. You can only ship the box via a courier service, but it will open and remove the contents of the box, if left unlocked.

Padlocks can only be opened by the corresponding key (not by another).

Assuming the courier service does not use any methods to open the lock or break the box, how can you get the secret document to that person? **(10 Pts.)**

**10)** How does PGP work? Please explain in details. **(10 Pts.)**

**11)** Why would you recommend using ssh instead of telnet? Why wouldn't you? Please use examples to support your arguments. **(5 Pts.)**

**12)** If we would assume OS = DB:

Explain the functions of a database rootkit. **(5 Pts.)**

**13)** What is a salt? Why should password hashes be salted? Against what type of attacks does this provide protection? **(10 Pts.)**

**14)** What is the problem in using pattern matching signatures with IDS/IDP devices? What is the security problem in using protocol level detection? **(5 Pts.)**

**15)** What is "zone transfer"? In which phase of an attack does an attacker usually use it? **(5 Pts.)**

**16)** How can phishing mails be used to exploit telephone banking? **(5 Pts.)**

**Good Luck!**
**Ertunga Arsal**