

# Tentti S-38.3153 Tietoliikenteen tietoturva

## Exam S-38.3153 Security of Communication Protocols

8.1.2009

Put your name, student number, course code and date to each exercise paper. This helps you to receive your credits in fast and reliable manner. Answers are accepted in Finnish, Swedish or in English. Answers are judged based on their quality and clarity. A short and down to the fact answer will get better points than an excursive one. You may explain things further but beware that errors may lower your points (even if they are in extra matter).

1. Tarkastele seuraavia tapauksia: perustele lyhyesti mitä tekisit tilanteen ratkaisemiseksi ja miksi (2 p/tapaus).  
Evaluate following cases: what would you do to resolve situation and why? (2 p/case) (6 p)
  - a) Yrityksessä käytettävästä tekstinkäsittelyohjelmasta on löytynyt vakava haavoittuvuus, johon ei ole korjausta saatavissa. Haavoittuvuutta hyödyntävä esimerkkikoodi on saatavissa verkosta. Yrityksen toimintaan kuuluu olennaisesti tarjousdokumenttien (yleensä k.o. ohjelmalla tehtyjen) käsittely. Mitä teet?  
A vulnerability has been found from the word processing software used by company. There is no patch available and proof-of-concept code is available from Internet. Handling word processing documents (often made with the program in question) is critical part for company. What you do?
  - b) Sattumalta käy ilmi, että eräs työntekijä on liittännyt yrityksen verkkoon luvattoman WLAN-tukiaseman. Sinun tehtäväsi on selvittää onko niitä muitakin. Mitä teet?  
It is found out by a change that some employee has installed a WLAN accesspoint on company network without permit. You are assigned to find out if there are more. What do you do?
  - c) Käytettyäsi luokkatilassa ollutta PC:tä poislähtiessäsi havaitset näppäimistöjohdossa epäilyttävän välipalikan. Mitä teet?  
After you finish using classroom PC you notice a suspicious device on keyboard cable. What you do? (6 p)
2. Verkkoturvallisuutta voidaan toteuttaa palomureilla ja IDS-järjestelmillä. Miltä uhilta ne suojaavat ja miten? (6 p)  
Network security can be implemented using firewalls and IDS systems. What threats they are designed to protect from and how?(6 p)
3. Miten salausta käytetään tietoliikenteessä? Millaisia vaatimuksia tietoliikennejärjestelmissä käytetyille salausjärjestelmille on? (6 p)  
How encryption is used in data communication? What kind of requirements there are for encryption systems used for communications(6 p)
4. Kuvaile UMTS:n turvajärjestelmät. Miksi GSM-yhteensopivuus heikentää turvallisuutta? (6 p)  
Describe UMTS security system. Why GSM compatibility weakens security (6 p)
5. Suunnittele protokollaa tiedon turvalliseen siirtämiseen useamman järjestelmän välillä. Mitä asioita sinun tulee ottaa huomioon? (6 p)  
You are designing a protocol for secure information transmit between multiple systems. What aspects you must take into account? (6 p)
6. Mitä kirjaa/joja ja materiaalia käytit opiskeluun (rehellinen vastaus ½ p)  
What book(s) and materials you used for studying (truthful answer ½ p)

Markus Peuhkuri