Tentti S-38.3153 Tietoliikenteen tietoturva
Exam S-38.3153 Security of Communication Protocols

7.5.2009

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. Ohessa lehtiartikkeli ja yrityksen raportti eräästä murrosta. Rikolliset ilmeisesti onnistuivat muuttamaan domainin nimipalvelimien rekisteröintitietoja ja täten kaappaamaan kaiken domainin liikenteen. Arvioi mekanismeja, jotka olisivat suojanneet käyttäjiä ja rekisteröintitietoja. Miksi käytetyt mekanismit eivät suojanneet? (6 p)
   Attached is a news article and company report about one system compromise. Criminals managed to chane name service registry information and then take hold all of domain traffic. Evaluate mechanisms that would have protected users and registry information. Why existing mechanisms did not provide protection? (6 p)
2. Turvamekanismit voivat perustua ensisijaisesti estämiseen, havaitsemiseen tai toipumiseen. Esitä kustakin tapauksesta havainnollinen ja perusteltu esimerkki.
   Security mechanisms can base primarily on prevention, detection or recovery. Present an example for each case with short reasoning. (6 p)
3. Explain Kerberos 5 authentication. Why there is not need to trust much on each computer? (6 p)
   Kuvaile Kerberos 5 autentikointi. Miksi jokaiseen koneeseen ei tarvitse luottaa täydellisesti? (6 p)
4. Selitä IPSec-arkkitehtuuri ja mekanismit. (6 p)
   Explain IPSec architecture and mechanisms. (6 p)
5. Millaisia käyttäjän autentikointimenetelmiä voidaan käyttää? Eroaako tilanne, jos tunnistaminen tapahtuu paikallisesti tai verkon yli? (6 p)
   What kind of authentication methods can be used? Is there a difference if authentication is done locally or over network?(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