Tietoturvan perusteet, erilliskoe 19.11.2010

Kirjoita jokaiseen vastauspaperiin kokeen nimi, pvm, oma nimesi, henkilötunnuksesi tai opiskelijanumerosi ja allekirjoituksesi. Numeroi sivut.

1. Esittele turvallisen suunnittelun kahdeksan periaatetta.
2. Kuvaile, mitä seuraavat virheillä tarkoitetaan, ja anna yksinkertainen esimerkki:

   a) Puskurin ylivuoto.

   b) Tietojen epätäydellinen välitys (incomplete mediation).

   c) Synkronointivirhe.

   d) SQL-solutus (SQL-injection).
3. Miksi salalohkot suositellaan ketjutettavaksi. Esittele ketjutusmenetelmät CBC ja Laskurimoodi. Analysoi yhden bitin tiedonsiirtovirheen vaikutusta vastaanottajalla. Tarvitseeko tällaisesta välittää, vai hoitaanko TCP pakettien saapumisen oikeanmuotoisena perille?
4. Piirrä seuraavat palomuuriratkaisut ja selitä niiden hyvät ja huonot puolet tai sovellustilanteet: yksinkertainen yhdyskäytävä, kaksoisyhdyskäytävä, rajoitusaliverkkopalomuuri.
5. Näytä, miten IPSec modifioi paketteja kuljetus- ja tunnelimoodissa. Piirrä tyypillen tilanne, jossa käytetään kuljetusmoodia. Tee vastaava tunnelimoodille.