

TLT-3301 Verkon Tietoturva  
Tentti 25.5.2010 TTY/TTFE/Tuure Vartiainen

1. Ovatko seuraavat väittämät totta vai tarua? Oikeasta vastauksesta saat +1 p, väärästä -1 p, tyhjäksi jätetystä 0 p. Maksimipisteet tästä tehtävästä siis 6 p, minimipistemäärä on 0 p.
  - a) Tietoturvallisuuden eri osa-alueet (fyysinenturvallisuus, henkilöstö-, ohjelmisto-, jne.) ovat riippuvaisia toisistaan.
  - b) Palomuri ei voi suodattaa verkkokerroksen (L3) paketteja kytkiessään kehyksiä linkkikerroksella (L2).
  - c) SNMP on usein verkonvalvontaa käytetty tietoliikenneprotokolla.
  - d) Passiiviselta tietoliikenteen salakuuntelulta on vaikeampi suojautua kuin aktiiviselta tietoliikenteen salakuuntelulta.
  - e) VPN-tunnelissa välitettävä liikenne on aina salattu salakuuntelijoilta.
  - f) Rikoslaisissa määritellyn tietomurron edellytyksenä on, että tietomurron tekijällä on tarkoitus aiheuttaa vahinkoa tai haittaa tietojenkäsittelylle tai tietojärjestelmän toiminnalle.
2. Minkälaisilla asioilla tietoliikenneverkon arkkitehtuuria ja topologiaa suunniteltaessa voidaan parantaa tietoliikenneverkon ja siihen liitettyjen tietojärjestelmien tietoturvan eri osa-alueita? (luottamuksellisuus, eheys ja saatavuus) (6 p.)
3. Identiteetin hallinta käsittää organisaation järjestelmissä ja verkoissa käytettävien käyttäjätunnusten ja -oikeuksien linkkaaren hallinnan. Mitä hyötyä tai haittaa identiteetin hallinnasta on verkon tietoturvaan ajatellen? (3 p.) Kerro mitä protokollia voidaan käyttää kertakirjautumisen toteuttamiseen ja mitä eroavaisuuksia niissä on? (3 p.)
4. Järjestelmän saatavuudella viitataan aikaan jonka järjestelmä on käyttäjien käytettävissä. Mitä tässä yhteydessä tarkoitetaan järjestelmän kahdentamisella ja mitä asioita kahdentamisessa tulee ottaa huomioon? (4 p.) Entä mitä tarkoitetaan lyhenteellä SLA ja kuinka saatavuus liittyy siihen? (2 p.)
5. Mitä on ICT-forensiikka? Miten eri ICT-forensiikkamenetelmiä voidaan jaotella ja miten kuvaamasi jaon mukaiset menetelmät eroavat toisistaan? Mikä on ICT-forensiikan merkitys tietoturvaloukkausten selvittämisessä? (6 p.)